

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
15 July 2004 (15.07.2004)

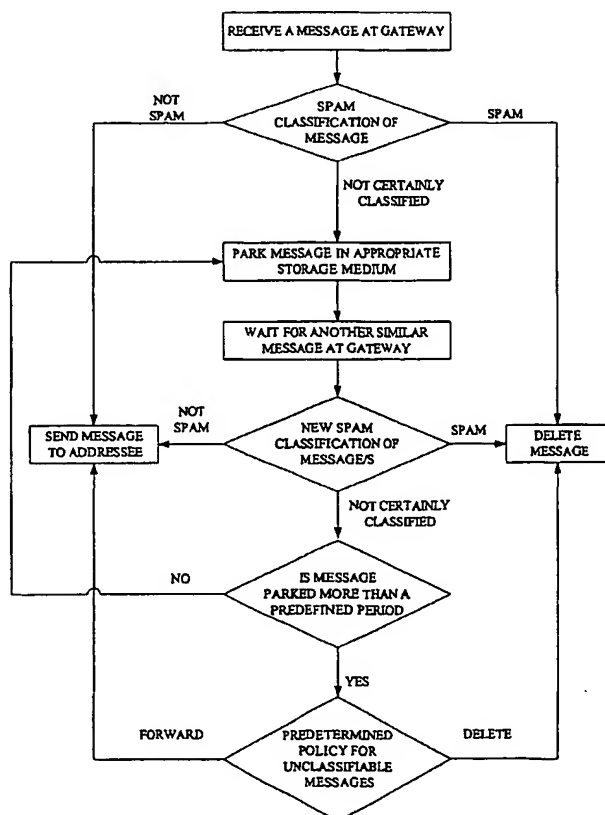
PCT

(10) International Publication Number  
**WO 2004/059506 A1**

- (51) International Patent Classification<sup>7</sup>: **G06F 15/173**, 11/30, 12/14, H04L 09/00, 09/32
- (21) International Application Number: **PCT/IL2003/001103**
- (22) International Filing Date: **25 December 2003 (25.12.2003)**
- (25) Filing Language: **English**
- (26) Publication Language: **English**
- (30) Priority Data:  
60/436,021 26 December 2002 (26.12.2002) US  
60/488,354 17 July 2003 (17.07.2003) US  
60/489,165 21 July 2003 (21.07.2003) US
- (71) Applicant (for all designated States except US): **COMM-TOUCH SOFTWARE LTD. [IL/IL]**; 1A Hatzoran Street, 42504 Netanya (IL).
- (72) Inventors; and  
(75) Inventors/Applicants (for US only): **TURGEMAN, Yehuda [IL/IL]**; 44851 Alfei Menashe (IL). **DRAI, David [IL/IL]**; 40300 Kfar Yona (IL). **LEV, Amir [IL/IL]**; 40696 Ein Vered (IL).
- (74) Agents: **SANFORD T. COLB & CO. et al.**; P.O. Box 2273, 76122 Rehovot (IL).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: **DETECTION AND PREVENTION OF SPAM**



(57) Abstract: A method and system for combating spam, including obtaining information contained in messages, employing a variable criteria to the information, encrypting at least part of the information employing a non-reversible encryption so as to generate encrypted information, transmitting at least the encrypted information to a server for spam indication thereby receiving from the server classification data and determining the spam classification of the messages at least partially based on the classification data.

WO 2004/059506 A1



European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

**Published:**

— *with international search report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

## DETECTION AND PREVENTION OF SPAM

5

## REFERENCE TO CO-PENDING APPLICATIONS

This application claims priority from the following co-pending U.S. Patent Applications:

U.S. Provisional application serial number 60/436,021, entitled  
10 "PREVENTION OF BULK TRANSMISSION OF OBJECTS IN A  
COMMUNICATION NETWORK", filed December 26, 2002, U.S. Provisional  
application serial number 60/488,354, entitled "DETECTION AND PREVENTION OF  
SPAM AND BULK MESSAGES", filed July 17, 2003, and U.S. Provisional  
application serial number 60/489,165, entitled "DETECTION AND PREVENTION OF  
15 SPAM AND BULK MESSAGES", filed July 21, 2003.

## FIELD OF THE INVENTION

The present invention relates to classification of messages in a  
20 communication network generally and more particularly to classification of messages as  
spam.

## BACKGROUND OF THE INVENTION

The following U.S. Patents are believed to represent the state of the art:  
25 6,330,590; 6,421,709; 6,453,327; 6,460,050 and 6,622,909.

## SUMMARY OF THE INVENTION

The present invention seeks to provide a method and system for detecting the bulk transmission of objects in a communication network and preventing or  
5 avoiding further transmission of these objects.

There is thus provided in accordance with a preferred embodiment of the present invention a method for combating spam including classifying a message at least partially by evaluating at least one message parameter, using at least one variable criterion, thereby providing a spam classification and handling the message based on the  
10 spam classification.

In accordance with another preferred embodiment of the present invention the at least one variable criterion includes a criterion which changes over time. Additionally or alternatively, the at least one variable criterion includes a parameter template-defined function.

15 There is also provided in accordance with another preferred embodiment of the present invention a method for combating spam including classifying messages at least partially by evaluating at least one message parameter of multiple messages, by employing at least one evaluation criterion which change over time, thereby providing spam classifications and handling the messages based on the spam classifications.

20 In accordance with another preferred embodiment of the present invention the classifying is at least partially responsive to similarities between plural messages among the multiple messages, which similarities are reflected in the at least one message parameter. Alternatively or additionally, the classifying is at least partially responsive to similarities between plural messages among the multiple messages, which  
25 similarities are reflected in outputs of applying the at least one evaluation criterion to the at least one message parameter. Alternatively or additionally, the classifying is at least partially responsive to similarities in multiple outputs of applying a single evaluation criterion to the at least one message parameter in multiple messages. In accordance with another preferred embodiment of the present invention the classifying  
30 is at least partially responsive to the extent of similarities between plural messages among the multiple messages which similarities are reflected in the at least one message parameter. Alternatively or additionally, the classifying is at least partially responsive to

the extent of similarities between plural messages among the multiple messages which similarities are reflected in outputs of applying the at least one evaluation criterion to the at least one message parameter. In accordance with yet another preferred embodiment of the present invention the classifying is at least partially responsive to the  
5 extent of similarities in multiple outputs of applying a single evaluation criterion to the at least one message parameter in multiple messages.

In accordance with still another preferred embodiment of the present invention the extent of similarities includes a count of messages among the multiple messages which are similar.

10 In accordance with another preferred embodiment of the present invention the classifying is at least partially responsive to similarities in outputs of applying evaluation criteria to the at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to the at least one message parameter in the multiple messages, yielding a corresponding plurality of  
15 outputs indicating a corresponding plurality of similarities among the multiple messages. Additionally, the classifying also includes aggregating individual similarities among the plurality of similarities. Additionally, the aggregating individual similarities among the plurality of similarities includes applying weights to the individual similarities. Alternatively, the aggregating individual similarities among the plurality of  
20 similarities includes calculating a polynomial over the individual similarities.

In accordance with yet another preferred embodiment of the present invention the classifying is at least partially responsive to extents of similarities in outputs of applying evaluation criteria to the at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to  
25 the at least one message parameter in the multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of extents of similarities among the multiple messages. Additionally, the classifying also includes aggregating individual extents of similarities among the plurality of extents of similarities. Additionally, the aggregating individual extents of similarities among the plurality of extents of  
30 similarities includes applying weights to the individual extents similarities. Alternatively, the aggregating individual extents of similarities among the plurality of

extents of similarities includes calculating a polynomial over the individual extents of similarities.

Preferably, the extents of similarities include a count of messages among the multiple messages which are similar.

5 In accordance with still another preferred embodiment of the present invention the criteria include a parameter template-defined function.

In accordance with another preferred embodiment of the present invention the classifying employs a function of outputs of evaluating at least one message parameter of the multiple messages. Additionally, the classifying is at least  
10 partially responsive to similarities between outputs of the evaluating at least one message parameter of multiple messages.

In accordance with yet another preferred embodiment of the present invention the classifying includes the using at least one variable criterion at at least one gateway and the providing spam classifications at at least one server, receiving  
15 evaluation outputs from the at least one gateway and providing the spam classifications to the at least one gateway. Additionally, the classifying also includes encrypting at least part of the evaluation outputs by employing a non-reversible encryption so as to generate encrypted information and transmitting at least the encrypted information to the at least one server.

20 In accordance with another preferred embodiment of the present invention the transmitting includes transmitting information of a length limited to a predefined threshold.

There is further provided in accordance with another preferred embodiment of the present invention a method for combating spam including  
25 categorizing incoming messages received at at least one gateway into at least first, second and third categories, providing spam classifications for incoming messages in at least the first and second categories, not immediately providing a spam classification for incoming messages in the third category, storing incoming messages in the third category and thereafter providing spam classifications for the incoming messages in the  
30 third category. In accordance with another preferred embodiment of the present invention the method also includes handling the incoming messages based on the spam classifications.

In accordance with another preferred embodiment of the present invention the providing a spam classification for the incoming messages in the third category also includes providing a spam classification for a second message received at the at least one gateway. In accordance with another preferred embodiment of the present invention the method also includes waiting up to a predetermined period of time between the providing spam classifications for incoming messages in at least the first and second categories and the thereafter providing a spam classification for the incoming messages in the third category.

In accordance with another preferred embodiment of the present invention the categorizing includes at least one of requesting feedback from an addressee of the messages, evaluating compliance of the messages with a predefined policy, evaluating registration status of at least one registered address in the messages, analyzing a match among network references in the messages, analyzing a match between at least one translatable address in the messages and at least one other network reference in the messages, at least partially actuating an unsubscribe feature in the messages, analyzing an unsubscribe feature in the messages, employing a variable criteria, sending information to a server and receiving categorization data based thereon, employing categorization data received from a server and employing stored categorization data.

There is yet further provided in accordance with another preferred embodiment of the present invention a method for combating spam including classifying a message at least partially by relating to an unsubscribe feature in the message, thereby providing spam classifications for the message and handling the message based on the spam classifications.

In accordance with another preferred embodiment of the present invention the classifying also includes identifying whether the message includes an unsubscribe feature. Alternatively or additionally, the classifying also includes identifying whether the unsubscribe feature includes a reference to an addressee of the message. Additionally, the reference to an addressee of the message includes an e-mail address. Alternatively, the reference to an addressee of the message includes a per-addressee generated ID. Additionally, the per-addressee generated ID includes a user identification number.

There is even further provided in accordance with yet another preferred embodiment of the present invention a method for combating spam including classifying a message at least partially by at least partially actuating an unsubscribe feature in the message, thereby providing spam classifications for the messages and  
5 handling the message based on the spam classifications.

In accordance with another preferred embodiment of the present invention the classifying includes analyzing an output of the at least partial actuating. Additionally, the analyzing an output of the at least partially actuating includes sensing whether part of the output indicates the occurrence of an error. In accordance with  
10 another preferred embodiment of the present invention the at least partially actuating also includes at least attempting communication with a network server.

In accordance with a preferred embodiment of the present invention the error indicates that the network server does not exist. Alternatively, the error indicates that the network server does not provide an unsubscribe functionality. Alternatively, the  
15 error indicates that the network server cannot unsubscribe a message addressee.

In accordance with another preferred embodiment of the present invention the analyzing an output of the at least partially actuating includes sensing whether part of the output includes an addressee reference. Preferably, the addressee reference includes an e-mail address. Alternatively, the addressee reference includes a  
20 per-addressee generated ID. Additionally, the per-addressee generated ID includes a user identification number.

In accordance with yet another preferred embodiment of the present invention the analyzing an output of the at least partially actuating also includes relating the addressee reference to at least one addressee reference characteristic of the message.  
25 Additionally, the at least one addressee reference characteristic of the message includes an e-mail address. Alternatively, the at least one addressee reference characteristic of the message includes a per-addressee generated ID. Additionally, the per- at least one addressee reference characteristic of the per-addressee generated ID includes a user identification number.

30 In accordance with another preferred embodiment of the present invention the classifying also includes recognizing the unsubscribe feature. Additionally, the recognizing the unsubscribe feature includes sensing a part of the



message including predefined keywords. Alternatively or additionally, the recognizing the unsubscribe feature includes sensing a part of the message including a network reference and a reference to an addressee of the messages. In accordance with another preferred embodiment of the present invention the network reference includes a  
5 reference to a network server. Additionally or alternatively, the reference to an addressee of the message includes an addressee e-mail address.

There is still further provided in accordance with another preferred embodiment of the present invention a method for combating spam including classifying a message at least partially by relating to registration status of at least one  
10 registered address in the message, thereby providing a spam classification for the message and handling the message based on the spam classifications.

In accordance with another preferred embodiment of the present invention the classifying includes employing a network service for determining the registration status. Additionally or alternatively, the registration status includes a  
15 registration date. Alternatively or additionally, the registration status includes a registration expiry date.

In accordance with another preferred embodiment of the present invention the classifying includes inspecting whether registration of the registered address has expired. Alternatively, the classifying includes inspecting whether the  
20 registered address has not been registered. In accordance with another preferred embodiment of the present invention the classifying includes comparing the registration date to a predefined date. In accordance with another preferred embodiment of the present invention the predefined date is a current date.

In accordance with a preferred embodiment of the present invention the  
25 registered address includes an Internet domain name. In accordance with another preferred embodiment of the present invention the Internet domain name is parked.

There is also provided in accordance with still another preferred embodiment of the present invention a method for combating spam including classifying a message at least partially by relating to a match among network references  
30 in the message, thereby providing a spam classification for the message and handling the message based on the spam classification.

In accordance with a preferred embodiment of the present invention the network references include at least one translatable network address and the match is between at least one translatable network address and another at least one of the network references. Additionally, the at least one translatable network address includes  
5 a registered network address. Alternatively, the at least one translatable network address includes an Internet domain name. In accordance with another preferred embodiment of the present invention the classifying also includes translating the translatable network address, thereby providing a translated network address.

In accordance with a preferred embodiment of the present invention the  
10 handling includes at least one of forwarding the message to an addressee of the message, storing the message in a predefined storage area, deleting the message, rejecting the message, sending the message to an originator of the message and delaying the message for a period of time and thereafter re-classifying the message.

Preferably, the message includes at least one of an e-mail, a network  
15 packet, a digital telecom message and an instant messaging message.

In accordance with another preferred embodiment of the present invention the classifying also includes at least one of requesting feedback from an addressee of the message, evaluating compliance of the message with a predefined policy, evaluating registration status of at least one registered address in the message,  
20 analyzing a match among network references in the message, analyzing a match between at least one translatable address in the message and at least one other network reference in the message, at least partially actuating an unsubscribe feature in the message, analyzing an unsubscribe feature in the message, employing a variable criteria, sending information to a server and receiving classification data based on the  
25 information, employing classification data received from a server and employing stored classification data.

There is further provided in accordance with another preferred embodiment of the present invention a system for combating spam including a message  
30 evaluator, operative to evaluate a message using at least one message parameter, the at least one message parameter including at least one variable criterion, a message classifier, operative to provide a spam classification of the message at least partially

based on an output of the message evaluator and a message handler, operative to handle the message based on the spam classification.

In accordance with a preferred embodiment of the present invention the at least one variable criterion includes a criterion which changes over time. Additionally  
5 or alternatively, the at least one variable criterion includes a parameter template-defined function.

There is yet further provided in accordance with yet another preferred embodiment of the present invention a system for combating spam including a message evaluator, operative to evaluate multiple messages using at least one message parameter  
10 of the multiple messages, the at least one message parameter including at least one variable criterion which changes over time, a message classifier, operative to provide spam classifications of the messages at least partially based on outputs of the message evaluator and a message handler, operative to handle the messages based on the spam classifications.

15 In accordance with a preferred embodiment of the present invention the spam classifications are at least partially based on similarities between plural messages among the multiple messages, which similarities are reflected in the at least one message parameter. Alternatively or additionally, the spam classifications are at least partially based on similarities between plural messages among the multiple messages,  
20 which similarities are reflected in outputs of applying the at least one evaluation criterion to the at least one message parameter. Alternatively or additionally, the spam classifications are at least partially based on similarities in multiple outputs of applying a single evaluation criterion to the at least one message parameter in multiple messages. In accordance with another preferred embodiment of the present invention the spam  
25 classifications are at least partially based on the extent of similarities between plural messages among the multiple messages which similarities are reflected in the at least one message parameter. Alternatively or additionally, the spam classifications are at least partially based on the extent of similarities between plural messages among the multiple messages which similarities are reflected in outputs of applying the at least one  
30 evaluation criterion to the at least one message parameter. In accordance with yet another preferred embodiment of the present invention the spam classifications are at

least partially based on the extent of similarities in multiple outputs of applying a single evaluation criterion to the at least one message parameter in multiple messages.

In accordance with another preferred embodiment of the present invention the extent of similarities includes a count of messages among the multiple  
5 messages which are similar.

In accordance with still another preferred embodiment of the present invention the spam classifications are at least partially based on similarities in outputs of applying evaluation criteria to the at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to the at least  
10 one message parameter in the multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of similarities among the multiple messages.

In accordance with a preferred embodiment of the present invention the system also includes an aggregator, operative to aggregate individual similarities among  
15 the plurality of similarities. Additionally, the aggregator is operative to apply a weighting to the individual similarities. Alternatively, the aggregator is operative to calculate a polynomial over the individual similarities.

In accordance with another preferred embodiment of the present invention the spam classifications are at least partially based on extents of similarities in  
20 outputs of applying evaluation criteria to the at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to the at least one message parameter in the multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of extents of similarities among the multiple messages. In accordance with yet another preferred embodiment of the  
25 present invention the message classifier also includes an aggregator, operative to aggregate individual extents of similarities among the plurality of extents of similarities. In accordance with still another preferred embodiment of the present invention the aggregator is operative to apply a weighting to the individual extents similarities. Alternatively, the aggregator is operative to calculate a polynomial over the individual  
30 extents of similarities.

In accordance with still another preferred embodiment of the present invention the extents of similarities include a count of messages among the multiple messages which are similar.

5 In accordance with a preferred embodiment of the present invention the at least one variable criterion includes a parameter template-defined function.

In accordance with yet another preferred embodiment of the present invention the message classifier is operative to employ a function of outputs of evaluating at least one message parameter of the multiple messages. Additionally, the spam classifications are at least partially based on similarities between outputs of the  
10 evaluating at least one message parameter of multiple messages.

In accordance with another preferred embodiment of the present invention the message evaluator includes at least one gateway and the message classifier includes at least one server and the at least one server is operative to receive the output from the at least one gateway and to provide the spam classification to the at least one  
15 gateway. Additionally, the at least one gateway also includes an encrypter, operative to encrypt at least part of the output by employing a non-reversible encryption so as to generate encrypted information and a transmitter, operative to transmit at least the encrypted information to the at least one server. In accordance with a preferred embodiment of the present invention the transmitter is operative to transmit information  
20 of a length limited to a predefined threshold.

There is even further provided in accordance with still another preferred embodiment of the present invention a system for combating spam including a message categorizer, operative to categorize incoming messages received at at least one gateway into at least first, second and third categories and a message classifier, operative to  
25 provide spam classifications for incoming messages in at least the first and second categories, the message classifier being operative to store incoming messages in the third category and at a time thereafter to provide spam classifications for the incoming messages in the third category.

In accordance with another preferred embodiment of the present  
30 invention the system also includes a message handler, operative to handle the incoming messages based on the spam classifications.

In accordance with yet another preferred embodiment of the present invention the message classifier is operative to provide a spam classification for a second message received at the at least one gateway at the time thereafter. In accordance with another preferred embodiment of the present invention the time  
5 thereafter includes a time not later than after a maximum predetermined waiting period.

There is also provided in accordance with another preferred embodiment of the present invention a system for combating spam including a message classifier, operative to provide a spam classification for a message at least partially by relating to an unsubscribe feature in the message and a message handler, operative to handle the  
10 message based on the spam classification.

In accordance with another preferred embodiment of the present invention the system also includes an unsubscribe identifier, operative to identify whether the message includes an unsubscribe feature.

In accordance with still another preferred embodiment of the present  
15 invention the system also includes an addressee identifier, operative to identify whether the unsubscribe feature includes a reference to an addressee of the message. In accordance with a preferred embodiment of the present invention the reference to an addressee of the message includes an e-mail address. Alternatively, the reference to an addressee of the message includes a per-addressee generated ID. Additionally, the per-  
20 addressee generated ID includes a user identification number.

There is further provided in accordance with another preferred embodiment of the present invention a system for combating spam including a message classifier, operative to provide a spam classification for a message at least partially by at least partial actuation of an unsubscribe feature in the message and a message handler,  
25 operative to handle the message based on the spam classification.

In accordance with another preferred embodiment of the present invention the system also includes an actuation analyzer operative to analyze an output of the at least partial actuation. Additionally, the analyzer is operative to sense whether part of the output indicates the occurrence of an error. In accordance with another  
30 preferred embodiment of the present invention the at least partial actuation also includes at least attempting communication with a network server. In accordance with a preferred embodiment of the present invention the error indicates that the network

server does not exist. Alternatively, the error indicates that the network server does not provide an unsubscribe functionality. Alternatively, the error indicates that the network server cannot unsubscribe a message addressee.

5 In accordance with another preferred embodiment of the present invention the analyzer is operative to sense whether part of the output includes an addressee reference. In accordance with a preferred embodiment of the present invention the addressee reference includes an e-mail address. Alternatively, the addressee reference includes a per-addressee generated ID. Additionally, the per-addressee generated ID includes a user identification number.

10 In accordance with another preferred embodiment of the present invention the analyzer is operative to relate the addressee reference to at least one addressee reference characteristic of the message. In accordance with another preferred embodiment of the present invention the at least one addressee reference characteristic of the message includes an e-mail address. Alternatively, the at least one addressee  
15 reference characteristic of the message includes a per-addressee generated ID. Additionally, the per- at least one addressee reference characteristic of the per-addressee generated ID includes a user identification number.

In accordance with another preferred embodiment of the present invention the system also includes an unsubscribe recognizer, operative to recognize the  
20 unsubscribe feature. Additionally, the unsubscribe recognizer is operative to sense a part of the message including predefined keywords. Additionally, the unsubscribe recognizer is operative to sense a part of the message including a network reference and a reference to an addressee of the messages. In accordance with a preferred embodiment of the present invention the network reference includes a reference to a network server.  
25 Alternatively or additionally, the reference to an addressee of the message includes an addressee e-mail address.

There is still further provided in accordance with yet another preferred embodiment of the present invention a system for combating spam including a message classifier, operative to provide a spam classification for a message at least partially by  
30 relating to registration status of at least one registered address in the message and a message handler, operative to handle the message based on the spam classifications.

In accordance with a preferred embodiment of the present invention the message classifier is operative to employ a network service for determining the registration status. Additionally or alternatively, the registration status includes a registration date. In accordance with a preferred embodiment of the present invention  
5 the registration status includes a registration expiry date.

In accordance with another preferred embodiment of the present invention the message classifier is operative to inspect whether registration of the registered address has expired. Alternatively or additionally, the message classifier is operative to inspect whether the registered address has not been registered.  
10 Additionally, the message classifier is operative to compare the registration date to a predefined date. In accordance with another preferred embodiment of the present invention the predefined date is a current date.

In accordance with another preferred embodiment of the present invention the registered address includes an Internet domain name. In accordance with  
15 another preferred embodiment of the present invention, the Internet domain name is parked.

There is yet further provided in accordance with another preferred embodiment of the present invention a system for combating spam including a message classifier, operative to provide a spam classification for a message at least partially by  
20 relating to a match among network references in the message and a message handler, operative to handle the message based on the spam classification.

In accordance with a preferred embodiment of the present invention the network references include at least one translatable network address and wherein the match is between at least one translatable network address and another at least one of  
25 the network references. Preferably, the at least one translatable network address includes a registered network address. Alternatively, the at least one translatable network address includes an Internet domain name.

In accordance with another preferred embodiment of the present invention the system also includes an address translator, operative to translate the  
30 translatable network address, thereby providing a translated network address.

In accordance with a preferred embodiment of the present invention the message handler is operative to perform at least one of the following: forward the



message to an addressee of the message, store the message in a predefined storage area, delete the message, reject the message, send the message to an originator of the message and delay the message for a period of time and thereafter re-classify the message.

5 In accordance with a preferred embodiment of the present invention the message includes at least one of: an e-mail, a network packet, a digital telecom message and an instant messaging message.

10 In accordance with a preferred embodiment of the present invention the message classifier is operative to provide the spam classification at least partially based on at least one of the following: feedback requested from an addressee of the message, compliance of the message with a predefined policy, a registration status of at least one  
15 registered address in the message, a match among network references in the message, a match between at least one translatable address in the message and at least one other network reference in the message, at least partial actuation an unsubscribe feature in the message, an analysis of an unsubscribe feature in the message, a variable criteria, information sent to a server and classification data received based on the information,  
classification data received from a server and stored classification data.

## BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in  
5 which:

Figs. 1A, 1B and 1C are simplified pictorial illustrations of a system and methodology for combating spam in accordance with a preferred embodiment of the present invention;

Fig. 1D is a simplified flowchart of the system and methodology of Figs.  
10 1A-1C;

Figs. 2A and 2B are simplified pictorial illustrations of a system and methodology for combating spam in accordance with a further preferred embodiment of the present invention;

Fig. 2C is a simplified flowchart of the system and methodology of Figs.  
15 2A and 2B;

Fig. 3 is a simplified pictorial illustration of a system and methodology for combating spam in accordance with yet a further preferred embodiment of the present invention;

Fig. 4 is a simplified pictorial illustration of a system and methodology  
20 for combating spam in accordance with a still further preferred embodiment of the present invention;

Fig. 5 is a simplified pictorial illustration of a system and methodology for combating spam in accordance with yet another preferred embodiment of the present invention; and

25 Fig. 6 is a simplified pictorial illustration of a system and methodology for combating spam in accordance with still another preferred embodiment of the present invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

It is appreciated that throughout the specification and claims the term "spam" refers to an unsolicited transmission of a message.

5           Reference is now made to Figs. 1A - 1D, which illustrate a system and methodology for combating spam in accordance with a preferred embodiment of the present invention. The system and methodology of the present invention employ an anti-spam technique which classifies incoming messages received at multiple gateways at a central server based on one or more message parameters, which parameters can be  
10           changed over time.

As seen in Fig. 1A, a spam detection server 100 updates, from time to time, a plurality of spam detection gateways 102 with parameter templates, such as parameter templates 104, 106 and 108.

It is appreciated that various types of parameter templates may be  
15           employed. For example, a template may include one or more of the following parameters: specific characters and/or words and/or character sequences at specific fixed or relative locations in the title, specific characters and/or words and/or character sequences at specific fixed or relative locations in the message body, e mail attributes in the body of the message, telephone number attributes in the body of the message, verbs  
20           in the body of the message and any other message attribute or part of a message attribute.

It is further appreciated that a relative location may be relative to any sub-object, such as a paragraph, a word or a formatting tag. It is also appreciated that a character sequence may be, for example, a fixed length sequence and/or a sequence  
25           delimited by a predetermined second character sequence and/or a sequence matching a pattern, such as a regular expression.

It is furthermore appreciated that a parameter template may also include instructions for calculating weightings and other values based on the various parameters.

30           One example of a parameter template, indicated in Fig. 1A by reference numeral 104, is as follows:

ADD THE NUMERICAL VALUE OF THE FIRST CHARACTER IN A MESSAGE BODY TO THE NUMERICAL VALUE OF THE THIRTIETH CHARACTER IN THE MESSAGE BODY;

CALCULATE THE SQUARE ROOT OF THE RESULT;

5           DIVIDE THE RESULT BY THE NUMERICAL VALUE OF THE FIFTEENTH CHARACTER IN THE MESSAGE BODY; AND

SET THE RESULT AS THE RESULT OF THE MESSAGE EXAMINATION.

Yet another example of a parameter template, indicated in Fig. 1A by  
10   reference numeral 106, is as follows:

CONCATENATE THE FIRST WORD OF THE THIRD PARAGRAPH OF A MESSAGE BODY AND THE THIRTIETH CHARACTER IN THE MESSAGE BODY;

CONCATENATE THE RESULT AND THE SECOND TELEPHONE  
15   NUMBER LOCATED IN THE MESSAGE BODY; AND

SET THE RESULT AS THE RESULT OF THE MESSAGE EXAMINATION.

Yet another example of a parameter template, indicated in Fig. 1A by  
reference numeral 108 is as follows:

20           LOCATE ALL NON-ALPHABETIC CHARACTERS IN A MESSAGE TITLE;

COUNT THE NUMBER OF CHARACTERS LOCATED; AND

SET THE RESULT AS THE RESULT OF THE MESSAGE EXAMINATION.

25           As seen in Fig. 1B, a message 110 received at a spam detection gateway 102 is examined based on at least one parameter template, such as any of templates 104, 106 or 108, which are updated from time to time by spam detection server 100. The result of the message examination is supplied by spam detection gateway 102 to spam detection server 100, which determines a spam classification for message 110.

30           The spam classification may be message examination result specific and/or may be message specific. It is appreciated that spam detection gateway 102 and/or spam detection server 100 may calculate weightings and other values based on

spam classifications of results of examination of a message according to multiple parameter templates to determine the spam classification of the message.

For examples, results of examination of a message according to parameter templates 104, 106 and 108 for message 110 may be 0.2, "Forp800-123-4567" and 5 respectively. The spam classification of these results may be low, high and medium respectively and a numerical representation of the spam classifications of these results may be 2, 9 and 6 on a 1 – 10 scale. By providing relative weighting to these spam classifications, server 100 may calculate the spam classification of message 110. The weighting for parameter templates 104, 106 and 108 may be 0.3, 0.5 and 0.2 respectively, and the spam classification of message 110 would therefore be  $2*0.3+9*0.5+6*0.2 = 6.1$  on a 1 – 10 scale.

Spam classifications and/or examination results and/or message attributes may be stored at the server 100, a gateway 102 or using any other storage functionality 112 and employed for examination and/or classification of later received messages, such as a message 113.

Additionally or alternatively, spam detection server 100 may transmit spam classifications to multiple ones of the plurality of spam detection gateways 102.

It is appreciated that according to a preferred embodiment of the present invention, a spam detection gateway 102 may employ a non-reversible encryption algorithm so as to generate an encrypted transformation of at least part of a message parameter. It is appreciated that the encrypted information may be shorter than any reversible transformation of at least part of a message parameter, so as to consume less network resources when transmitted through a network. It is further appreciated that the encrypted information is incomprehensible to spam detection server 100 so as to avoid revealing any confidential information contained in a message. It is further appreciated that the amount of information transmitted from a gateway 102 to server 100 may be limited according to a predefined threshold.

Based on a spam classification of a message, spam detection gateway 102 may perform any one or more of the following actions with the message 110: a message having low spam certainty may be forwarded to an addressee, such as a user 114, a message having high spam certainty may be deleted, as indicated by being sent to a symbolic trash bin 116, and a message having intermediate spam certainty may be

parked in an appropriate storage medium 118 until an appropriate later time when a new classification is made automatically or as the result of manual inspection by an administrator 120.

5 It is further appreciated that spam detection server 100 may make spam determinations by correlating the results of examination of a multiplicity of messages received by gateways 102 using a single or multiple parameter templates. High correlations tend to indicate the existence of spam and result in a spam classification being sent by server 100 to gateways 102.

10 It is appreciated that spam detection server 100 may employ any one or more of the following methods to correlate results of examination: an exact match, an approximate match and a cross-match. The spam detection server 100 may employ any other suitable correlation method. An exact match may be determined by comparing each character of a string representation of a result of examination for a first message with the character in the same position of the string representation of a result of  
15 examination for a second message. It is further appreciated that if all the comparisons are positive, the results match. Alternatively or additionally, an exact match may be determined by comparing a value calculated by applying a non-reversible encryption function to a result of examination of a first message and a non-reversible encryption function to a result of examination of a second message. Alternatively or additionally,  
20 an exact match may be determined by comparing any suitable one-to-one transformations of a result of examination of a first message with a one-to-one transformation of a result of examination of a second message.

It is appreciated that an approximate match may be determined by comparing an equivalent of a result of examination of a first message to an equivalent of  
25 a result of examination of a second message. Alternatively or additionally, an approximate match may be determined by comparing any suitable many-to-many transformation of a result of examination of a first message with a many-to-many transformation of a result of examination of a second message.

It is appreciated that a cross-match may be determined by comparing any  
30 suitable transformation of a result of examination of a first message using a first parameter template with a suitable transformation of a result of examination of a second message using a second parameter template.

Referring to Fig. 1C, another example of a parameter template 128 may be:

CONCATENATING THE WORD "FREE" IF IT EXISTS IN A MESSAGE TITLE AND THE FIRST TELEPHONE NUMBER LOCATED IN THE MESSAGE BODY.

5           As further seen in Fig. 1C, if spam detection gateway 102 receives non-identical messages 130, 132 and 134, notwithstanding the differences in the messages 130, 132 and 134 the result of examination thereof may yield identical calculated values. In the event that a significant number of messages having this calculated value are received within a predetermined time, gateway 102 classifies all of these messages,  
10 notwithstanding their differences, as being spam.

It is appreciated that spam detection gateway 102 need not be located along the original route of a message. A message may be redirected to spam detection gateway 102 by any suitable gateway through which the message passes. Additionally or alternatively, a gateway may send a copy of the message to gateway 102.

15           Reference is now made to Fig. 1D, which is a simplified flowchart illustrating the functionality of the embodiment of Figs. 1A - 1C. As seen in Fig. 1D, spam determination server 100 may be employed to define parameter templates which may change over time and which may additionally specify calculations to be performed by spam detection gateways 102. Updated parameter templates are provided from time  
20 to time to multiple gateways 102, which receive a multiplicity of incoming messages. The gateways 102 inspect the incoming messages using the current parameter templates and perform calculations specified by the templates.

Results of the examination are transmitted by the spam detection gateways 102 to the spam detection server 100, which may correlate the results received  
25 in respect of plural messages from multiple servers and which provides spam classifications, which are supplied to the spam detection gateways 102.

The individual gateways employ the spam classifications to discard an incoming message, send it to its addressee or handle it in any other suitable manner, as described hereinabove. The spam detection server updates the parameter templates from  
30 time to time, based inter alia on its experience with earlier incoming messages. It is appreciated that the embodiment of Figs. 1A - 1D is also applicable to a single gateway architecture. In such a case, changeable templates may be generated at the gateway and

spam determinations may be made thereby without involvement of an external server, preferably based on correlations between multiple messages received at that gateway. Inputs from other gateways may also be employed.

Reference is now made to Figs. 2A and 2B, which together illustrate a  
5 system and methodology for combating spam in accordance with another preferred embodiment of the present invention. The system and methodology of this embodiment of the present invention employ another anti-spam technique, wherein suspect messages are "parked", until further information which could assist in their classification becomes available. Fig. 2A illustrates receipt of three different types of messages 200, 202 and  
10 204 via a network 206 by a spam classification gateway 210. Gateway 210 is operative to classify messages 200, 202 and 204, based on any appropriate method as described hereinbelow, and to take appropriate action with respect thereto. In the illustrated example, message 200 is classified by gateway 210 as being legitimate and is sent without delay through gateway 210 to an addressee, such as a user 212. Message 202 is  
15 classified by gateway 210 as being spam and is deleted by the gateway 210, as indicated by being sent to a symbolic trashcan 214. Message 204, which cannot be classified with acceptable certainty according to appropriate criteria based on the information available at gateway 210, is stored or "parked" on a suitable storage medium, such as a file server, symbolized by the P sign 216.

20 Examples of an appropriate method employed by gateway 210 may include any one or more of the following, optionally together with one or more methodologies described hereinabove with reference to Figs. 1A - 1D: analysis of the message content; analysis of the message header; transmission of the message and/or parts of it, preferably in non-reversible encrypted form, to a server; determination of  
25 compliance of the message content and/or the message headers with a predefined policy and requesting feedback from the message addressee.

Within a suitable time, such as one hour, as indicated in Fig. 2B, if further information, such as a similar message 220 is received at the gateway 210, a decision may be made based on appropriate criteria to delete both message 204 and  
30 subsequently received message 220. Alternatively, a decision may be made at any suitable time based on appropriate criteria to send message 204 to an addressee, such as user 212 (Fig. 2A), or to send the message for further evaluation.



Based on a spam classification of a message, spam detection gateway 210 may perform any one or more of the following actions with a message: a message having low spam certainty may be forwarded to addressee, such as user 212 (Fig. 2A), a message having high spam certainty may be deleted, as indicated by being sent to a symbolic trash bin 214, and a message having intermediate spam certainty may be parked in an appropriate storage medium 216 until an appropriate later time when a new classification is made automatically or as the result of manual inspection by an administrator 222.

Reference is now made to Fig. 2C, which illustrates the operation of the functionality of the embodiment of Figs. 2A & 2B. Spam classification gateway 210 receives a message and preferably performs a classification triage. If the message is classified as spam it is deleted and if the message is classified as not being spam it is sent to the message addressee. If a sufficiently definite classification of a message is not possible, the message is preferably parked in an appropriate storage medium while further messages may be awaited.

The parked message and subsequently received messages, if any, may be again spam classified preferably in a classification triage. If the message is classified as spam, it is deleted and if the message is classified as not being spam it is sent to the message addressee. If a sufficiently definite classification of a message is not possible, the message is preferably parked in an appropriate storage medium while further messages are awaited. Should the accumulated parking time of a given message exceed a predetermined threshold, the message is handled according to a predetermined policy for unclassifiable messages and either deleted or sent to the addressee in accordance with that policy.

Reference is now made to Fig. 3, which illustrates a system and methodology for combating spam in accordance with yet another preferred embodiment of the present invention. The system and methodology of this embodiment of the present invention employ a further anti-spam technique in accordance with the present invention, wherein messages containing various types of 'unsubscribe' functionalities are classified by a spam inspecting gateway 300. As seen in Fig. 3, a first message 302, having a general unsubscribe feature 304, which does not contain any information regarding the message addressee, is classified by spam inspecting gateway 300 as

having a high likelihood of being spam and is therefore discarded, as indicated by being sent to a symbolic trash can 306. A second message 308, having an unsubscribe feature 310 which includes an addressee's email address, is classified by gateway 300 as having an intermediate likelihood of being spam and is sent to a temporary storage location, symbolized by server 312, to await manual classification by an email administrator. The presence of the addressee's email address may indicate the existence of a recipient database which is not characteristic of spam. A third message 314, having an unsubscribe feature 316 which includes a user identification number, is presumed to indicate the existence of a user database and is therefore presumed not to be spam. This message is therefore sent to an addressee, such as a user 318.

The foregoing methodology may be combined with any one or more of the methodologies described hereinabove with reference to Figs. 1A - 2C.

It is further appreciated that the unsubscribe feature in a message may include a network reference, such an address of a web service which enables a user to be removed from a list generating the message and/or from other address lists. Alternatively or additionally, an unsubscribe functionality include a mail address to which an unsubscribe request may be sent in order to remove the user from a mailing list generating the message and/or from other address lists.

It is further appreciated that an unsubscribe feature may be identified by locating predefined keywords in a message. Examples of a typical predefined keyword may include "unsubscribe", "exclude", "future mailing" and any other suitable keyword. Alternatively or additionally, an unsubscribe feature may be identified by a reference to a message addressee.

Reference is now made to Fig. 4, which illustrates a system and methodology for combating spam in accordance with yet another preferred embodiment of the present invention. The system and methodology of this embodiment of the present invention employ an additional anti-spam technique related to the presence of unsubscribe functionality in incoming messages. A spam inspecting gateway 400 inspects an incoming message 402 having an unsubscribe feature 404 in order to determine a spam classification of the message. The inspecting gateway 400 initially actuates the unsubscribe feature by communicating with a server 406 which is typically addressed by the unsubscribe feature 404. A spam classification is determined based on

a response received from server 406. In the illustrated example, receipt of an error response indicating that the unsubscribe function does not exist may indicate a relatively high spam certainty. An error response indicating that the unsubscribe function does exist but is not operating properly may indicate an intermediate spam certainty and an error message indicating successful initial actuation of the unsubscribe function may  
5 indicate a relatively low spam certainty, without actually causing the addressee to be unsubscribed.

The foregoing methodology may be combined with any one or more of the methodologies described hereinabove with reference to Figs. 1A - 3.

10 Based on a spam classification of a message, spam inspecting gateway 400 may perform any one or more of the following actions with a message: a message having low spam certainty may be forwarded to addressee, such as a user 414, a message having high spam certainty may be deleted, as indicated by being sent to a symbolic trash bin 416, and a message having intermediate spam certainty may be  
15 parked in an appropriate storage medium 418 until an appropriate later time when a new classification is made automatically or as the result of manual inspection by an administrator 420.

It is further appreciated that the unsubscribe feature in a message may include a network reference, such an address of a web service which enables a user to  
20 be removed from a list generating the message and/or from other address lists. Alternatively or additionally, an unsubscribe functionality may include a mail address to which an unsubscribe request may be sent in order to remove the user from a mailing list generating the message and/or from other address lists.

It is further appreciated that an unsubscribe feature may be identified by  
25 locating predefined keywords in a message. Examples of a typical predefined keyword may include "unsubscribe", "exclude", "future mailing" and any other suitable keyword. Alternatively or additionally, an unsubscribe feature may be identified by a reference to a message addressee.

Reference is now made to Fig. 5, which illustrates a system and  
30 methodology for combating spam in accordance with yet another preferred embodiment of the present invention. The system and methodology of this embodiment of the present invention employ an additional anti-spam technique related to registration status

of the domain name or any other registered address in an incoming message. An inspector gateway 500 inspects an incoming message 502 having a domain indication 504 or any other registered address. The inspector gateway 500 may employ a look up directory such as directory 506 to check the registration date 508 and/or the expiry date 508 of the domain indication 504. Relatively newly registered addresses may indicate a high certainty of spam. Additionally or alternatively, a registered address for which registration has expired may indicate a high certainty of spam. Additionally or alternatively, a parked status, as explained below, may indicate a higher level of indication of spam.

10           The foregoing methodology may be combined with any one or more of the methodologies described hereinabove with reference to Figs. 1A - 4.

          A message having low spam certainty may be forwarded to addressee, such as a user 514, a message having high spam certainty may be deleted, as indicated by being sent to a symbolic trash bin 516, and a message having intermediate spam 15 certainty may be parked in an appropriate storage medium 518 until an appropriate later time when a new classification is made automatically or as the result of manual inspection by an administrator 520.

          It is further appreciated that a registered network address may be a network reference at least a part of which requires registration at a registry prior to use. 20 A registered network address may be an Internet domain name and/or any network address that comprises an Internet domain name, such as an Internet e-mail address or a URL. An expired registered address may be a registered address for which a periodic registration was required and was not performed. It is further appreciated that the registration date of a registered network address may be the date on which the address 25 was first registered. The term "parked status" typically refers to a domain that was registered but does not refer to an operative web site.

          Reference is now made to Fig. 6, which illustrates a system and methodology for combating spam in accordance with yet another preferred embodiment of the present invention. The system and methodology of this embodiment of the 30 present invention employ an additional anti-spam technique related to matching of various addresses appearing in an incoming message. An inspector gateway 600 inspects an incoming message 602 having a domain name indication 604 or any other

translatable reference and at least one other reference, such as IP address 606. The inspector gateway 600 may employ a look up directory 608 to translate the domain name indication 604 and/or any other translatable reference and then may compare one or more translated references to any one or more references and/or other translated references in message 602 in order to ascertain the presence of matches. Matches indicate a relatively low spam certainty.

The foregoing methodology may be combined with any one or more of the methodologies described hereinabove with reference to Figs. 1A - 5.

A message having low spam certainty may be forwarded to addressee, such as a user 614, a message having high spam certainty may be deleted, as indicated by being sent to a symbolic trash bin 616, and a message having intermediate spam certainty may be parked in an appropriate storage medium 618 until an appropriate later time when a new classification is made automatically or as the result of manual inspection by an administrator 620.

It is further appreciated that a translatable reference may be a reference at least a part of which may be translated by querying a translation service. A symbolic Internet host name, for example, can be translated to a numeric IP address by employing an Internet domain registry service. As another example, a translatable reference may be any network address including a symbolic Internet host name such as an e-mail address or a URL.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove as well as variations and modifications which would occur to persons skilled in the art upon reading the specification and which are not in the prior art.

## CLAIMS

1. A method for combating spam comprising:  
classifying a message at least partially by evaluating at least one message  
5 parameter, using at least one variable criterion, thereby providing a spam classification;  
and  
handling said message based on said spam classification.
2. A method for combating spam according to claim 1 and wherein said at  
10 least one variable criterion comprises a criterion which changes over time.
3. A method for combating spam according to claim 1 or claim 2 and  
wherein said at least one variable criterion comprises a parameter template-defined  
function.  
15
4. A method for combating spam according to any of claims 1 - 3 and  
wherein said classifying comprises:  
said using at least one variable criterion at at least one gateway; and  
said providing spam classifications at at least one server, receiving  
20 evaluation outputs from said at least one gateway and providing said spam  
classifications to said at least one gateway.
5. A method for combating spam according to claim 4 and wherein said  
classifying also comprises:  
25 encrypting at least part of said evaluation outputs by employing a non-  
reversible encryption so as to generate encrypted information; and  
transmitting at least said encrypted information to said at least one server.
6. A method for combating spam according to claim 5 and wherein said  
30 transmitting comprises transmitting information of a length limited to a predefined  
threshold.

7. A method for combating spam according to any of claims 1 - 6 and wherein said handling comprises at least one of:
- forwarding said message to an addressee of said message;
  - storing said message in a predefined storage area;
  - 5 deleting said message;
  - rejecting said message;
  - sending said message to an originator of said message; and
  - delaying said message for a period of time and thereafter re-classifying said message.
- 10
8. A method for combating spam according to any of claims 1 - 7 and wherein said message comprises at least one of:
- an e-mail;
  - a network packet;
  - 15 a digital telecom message; and
  - an instant messaging message.
9. A method for combating spam according to any of claims 1 - 8 and wherein said classifying also comprises at least one of:
- 20 requesting feedback from an addressee of said message;
  - evaluating compliance of said message with a predefined policy;
  - evaluating registration status of at least one registered address in said message;
  - analyzing a match among network references in said message;
  - 25 analyzing a match between at least one translatable address in said message and at least one other network reference in said message;
  - at least partially actuating an unsubscribe feature in said message;
  - analyzing an unsubscribe feature in said message;
  - employing a variable criteria;
  - 30 sending information to a server and receiving classification data based on said information;
  - employing classification data received from a server; and

employing stored classification data.

10. A method for combating spam comprising:  
classifying messages at least partially by evaluating at least one message  
5 parameter of multiple messages, by employing at least one evaluation criterion which  
changes over time, thereby providing spam classifications; and  
handling said messages based on said spam classifications.
11. A method for combating spam according to claim 10 and wherein said  
10 classifying is at least partially responsive to similarities between plural messages among  
said multiple messages, which similarities are reflected in said at least one message  
parameter.
12. A method for combating spam according to claim 10 or claim 11 and  
15 wherein said classifying is at least partially responsive to similarities between plural  
messages among said multiple messages, which similarities are reflected in outputs of  
applying said at least one evaluation criterion to said at least one message parameter.
13. A method for combating spam according to any of claims 10 - 12 and  
20 wherein said classifying is at least partially responsive to similarities in multiple outputs  
of applying a single evaluation criterion to said at least one message parameter in  
multiple messages.
14. A method for combating spam according to any of claims 10 - 13 and  
25 wherein said classifying is at least partially responsive to the extent of similarities  
between plural messages among said multiple messages which similarities are reflected  
in said at least one message parameter.
15. A method for combating spam according to any of claims 10 - 14 and  
30 wherein said classifying is at least partially responsive to the extent of similarities  
between plural messages among said multiple messages which similarities are reflected



in outputs of applying said at least one evaluation criterion to said at least one message parameter.

16. A method for combating spam according to any of claims 10 - 15 and  
5 wherein said classifying is at least partially responsive to the extent of similarities in multiple outputs of applying a single evaluation criterion to said at least one message parameter in multiple messages.

17. A method for combating spam according to any of claims 14 - 16 and  
10 wherein said extent of similarities comprises a count of messages among said multiple messages which are similar.

18. A method for combating spam according to any of claims 10 - 17 and  
wherein said classifying is at least partially responsive to similarities in outputs of  
15 applying evaluation criteria to said at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to said at least one message parameter in said multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of similarities among said multiple messages.

20 19. A method according to claim 18 and wherein said classifying also comprises aggregating individual similarities among said plurality of similarities.

20. A method according to claim 19 and wherein said aggregating individual  
25 similarities among said plurality of similarities comprises applying weights to said individual similarities.

21. A method according to claim 19 and wherein said aggregating individual  
similarities among said plurality of similarities comprises calculating a polynomial over  
30 said individual similarities.

22. A method for combating spam according to any of claims 10 - 21 and wherein said classifying is at least partially responsive to extents of similarities in outputs of applying evaluation criteria to said at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to  
5 said at least one message parameter in said multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of extents of similarities among said multiple messages.
23. A method according to claim 22 and wherein said classifying also  
10 comprises aggregating individual extents of similarities among said plurality of extents of similarities.
24. A method according to claim 23 and wherein said aggregating individual  
15 extents of similarities among said plurality of extents of similarities comprises applying weights to said individual extents similarities.
25. A method according to claim 23 and wherein said aggregating individual  
extents of similarities among said plurality of extents of similarities comprises  
calculating a polynomial over said individual extents of similarities.  
20
26. A method for combating spam according to any of claims 22 - 25 and  
wherein said extents of similarities comprises a count of messages among said multiple  
messages which are similar.
- 25 27. A method for combating spam according to any of claims 10 - 26 and  
wherein said at least one evaluation criterion comprises a parameter template-defined  
function.
28. A method for combating spam according to any of claims 10 - 27 and  
30 wherein said classifying employs a function of outputs of evaluating at least one  
message parameter of said multiple messages

29. A method for combating spam according to claim 28 and wherein said classifying is at least partially responsive to similarities between outputs of said evaluating at least one message parameter of multiple messages.

5 30. A method for combating spam according to any of claims 10 - 29 and wherein said classifying comprises:  
said evaluating at at least one gateway; and  
said providing spam classifications at at least one server, receiving  
evaluation outputs from said at least one gateway and providing said spam  
10 classifications to said at least one gateway.

31. A method for combating spam according to claim 30 and wherein said classifying also comprises:  
encrypting at least part of said evaluation outputs by employing a non-  
15 reversible encryption so as to generate encrypted information; and  
transmitting at least said encrypted information to said at least one server.

32. A method for combating spam according to claim 31 and wherein said transmitting comprises transmitting information of a length limited to a predefined  
20 threshold.

33. A method for combating spam according to any of claims 10 - 32 and wherein said handling comprises at least one of:  
forwarding said messages to addressees of said messages;  
25 storing said messages in a predefined storage area;  
deleting said messages;  
rejecting said messages;  
sending said messages to originators of said messages; and  
delaying said messages for a period of time and thereafter re-classifying  
30 said messages.

34. A method for combating spam according to any of claims 10 - 33 and wherein said messages comprise at least one of:

an e-mail;  
network packets;  
5 digital telecom messages; and  
instant messaging messages.

35. A method for combating spam according to any of claims 10 - 34 and wherein said classifying also comprises at least one of:

10 requesting feedback from an addressee of said messages;  
evaluating compliance of said messages with a predefined policy;  
evaluating registration status of at least one registered address in said  
messages;  
analyzing a match among network references in said messages  
15 analyzing a match between at least one translatable address in said  
messages and at least one other network reference in said messages;  
at least partially actuating an unsubscribe feature in said messages;  
analyzing an unsubscribe feature in said messages;  
employing a variable criteria;  
20 sending information to a server and receiving classification data based  
thereon;  
employing classification data received from a server; and  
employing stored classification data.

25 36. A method for combating spam comprising:  
categorizing incoming messages received at at least one gateway into at  
least first, second and third categories;  
providing spam classifications for incoming messages in at least said first  
and second categories;  
30 not immediately providing a spam classification for incoming messages  
in said third category;  
storing incoming messages in said third category; and

thereafter providing spam classifications for said incoming messages in said third category.

37. A method for combating spam according to claim 36 and also  
5 comprising:

handling said incoming messages based on said spam classifications.

38. A method for combating spam according to claim 37 and wherein said  
handling comprises one or more of:

10 forwarding said messages to addressees of said messages;  
storing said messages in a predefined storage area;  
deleting said messages;  
rejecting said messages;  
sending said messages to originators of said messages; and  
15 delaying said messages for a period of time and thereafter re-classifying  
said messages.

39. A method for combating spam according to any of claims 36 - 38 and  
wherein said providing a spam classification for said incoming messages in said third  
20 category also comprises providing a spam classification for a second message received  
at said at least one gateway.

40. A method for combating spam according to any of claims 36 - 39 and  
also comprising waiting up to a predetermined period of time between said providing  
25 spam classifications for incoming messages in at least said first and second categories  
and said thereafter providing a spam classification for said incoming messages in said  
third category.

41. A method for combating spam according to any of claims 36 - 40 and  
30 wherein said incoming messages comprise at least one of:

e-mail messages;  
network packets;

digital telecom messages; and  
instant messaging messages.

42. A method for combating spam according to any of claims 36 – 41 and  
5 wherein said categorizing comprises at least one of:  
requesting feedback from an addressee of said messages;  
evaluating compliance of said messages with a predefined policy;  
evaluating registration status of at least one registered address in said  
messages;  
10 analyzing a match among network references in said messages  
analyzing a match between at least one translatable address in said  
messages and at least one other network reference in said messages;  
at least partially actuating an unsubscribe feature in said messages;  
analyzing an unsubscribe feature in said messages;  
15 employing a variable criteria;  
sending information to a server and receiving categorization data based  
thereon;  
employing categorization data received from a server; and  
employing stored categorization data.  
20
43. A method for combating spam according to any of claims 36 – 41 and  
wherein said providing spam classifications comprises at least one of:  
requesting feedback from an addressee of said messages;  
evaluating compliance of said messages with a predefined policy;  
25 evaluating registration status of at least one registered address in said  
messages;  
analyzing a match among network references in said messages  
analyzing a match between at least one translatable address in said  
messages and at least one other network reference in said messages;  
30 at least partially actuating an unsubscribe feature in said messages;  
analyzing an unsubscribe feature in said messages;  
employing a variable criteria;

sending information to a server and receiving classification data based thereon;

employing classification data received from a server; and  
employing stored classification data.

5

44. A method for combating spam comprising:  
classifying a message at least partially by relating to an unsubscribe feature in the message, thereby providing spam classifications for said message; and  
handling said message based on said spam classifications.

10

45. A method for combating spam according to claim 44 and wherein said classifying also comprises identifying whether said message includes an unsubscribe feature.

15

46. A method for combating spam according to claim 44 or claim 45 and wherein said classifying also comprises identifying whether said unsubscribe feature includes a reference to an addressee of said message.

20

47. A method for combating spam according to claim 46 and wherein said reference to an addressee of said message comprises an e-mail address.

48. A method for combating spam according to claim 46 and wherein said reference to an addressee of said message comprises a per-addressee generated ID.

25

49. A method for combating spam according to claim 48 and wherein said per-addressee generated ID comprises a user identification number.

50. A method for combating spam comprising:  
classifying a message at least partially by at least partially actuating an unsubscribe feature in the message, thereby providing spam classifications for said messages; and

30

handling said message based on said spam classifications.

51. A method for combating spam according to claim 50 and wherein said classifying comprises analyzing an output of said at least partial actuation.

5 52. A method for combating spam according to claim 51 and wherein said analyzing an output of said at least partially actuating comprising sensing whether part of said output indicates the occurrence of an error.

53. A method for combating spam according to claim 52 and wherein said at  
10 least partially actuating also comprises at least attempting communication with a network server.

54. A method for combating spam according to claim 53 and wherein said error indicates that said network server does not exist.

15

55. A method for combating spam according to claim 53 and wherein said error indicates that said network server does not provide an unsubscribe functionality.

56. A method for combating spam according to claim 53 and wherein said  
20 error indicates that said network server cannot unsubscribe a message addressee.

57. A method for combating spam according to claim 51 and wherein said analyzing an output of said at least partially actuating comprises sensing whether part of said output comprises an addressee reference.

25

58. A method for combating spam according to claim 57 and wherein said addressee reference comprises an e-mail address.

59. A method for combating spam according to claim 57 and wherein said  
30 addressee reference comprises a per-addressee generated ID.



60. A method for combating spam according to claim 59 and wherein said per-addressee generated ID comprises a user identification number.

61. A method for combating spam according to any of claims 57 - 60 and  
5 wherein said analyzing an output of said at least partially actuating also comprises relating said addressee reference to at least one addressee reference characteristic of said message.

62. A method for combating spam according to claim 61 and wherein said at  
10 least one addressee reference characteristic of said message comprises an e-mail address.

63. A method for combating spam according to claim 61 and wherein said at  
15 least one addressee reference characteristic of said message comprises a per-addressee generated ID.

64. A method for combating spam according to claim 63 and wherein said  
20 per- at least one addressee reference characteristic of said per-addressee generated ID comprises a user identification number.

65. A method for combating spam according to any of claims 44 - 64 and  
wherein said classifying also comprises recognizing said unsubscribe feature.

66. A method for combating spam according to claim 65 and wherein said  
25 recognizing said unsubscribe feature comprises sensing a part of said message comprising predefined keywords.

67. A method for combating spam according to claim 65 and wherein said  
30 recognizing said unsubscribe feature comprises sensing a part of said message comprising a network reference and a reference to an addressee of said messages.

68. A method for combating spam according to claim 67 and wherein said network reference comprises a reference to a network server.

69. A method for combating spam according to claim 67 or claim 68 and  
5 wherein said reference to an addressee of said message comprises an addressee e-mail address.

70. A method for combating spam according to any of claims 44 – 69 and wherein said handling comprises one or more of:  
10 forwarding said message to an addressee of said message;  
storing said message in a predefined storage area;  
deleting said message;  
rejecting said message;  
sending said message to an originator of said message; and  
15 delaying said message for a period of time and thereafter re-classifying said message.

71. A method for combating spam according to any of claims 44 –70 and wherein said message comprises at least one of:  
20 an e-mail;  
a network packet;  
a digital telecom message; and  
an instant messaging message.

25 72. A method for combating spam according to any of claims 44 –71 and wherein said classifying also comprises at least one of:  
requesting feedback from an addressee of said message;  
evaluating compliance of said message with a predefined policy;  
evaluating registration status of at least one registered address in said  
30 message;  
analyzing a match among network references in said message;

analyzing a match between at least one translatable address in said message and at least one other network reference in said message;

at least partially actuating an unsubscribe feature in said message;

analyzing an unsubscribe feature in said message;

5 employing a variable criteria;

sending information to a server and receiving classification data based thereon;

employing classification data received from a server; and

employing stored classification data.

10

73. A method for combating spam comprising:

classifying a message at least partially by relating to registration status of at least one registered address in said message, thereby providing a spam classification for said message; and

15 handling said message based on said spam classifications.

74. A method for combating spam according to claim 73 and wherein said classifying comprises employing a network service for determining said registration status.

20

75. A method for combating spam according to claim 73 or claim 74 and wherein said registration status comprises a registration date.

76. A method for combating spam according to claim 73 or claim 74 and  
25 wherein said registration status comprises a registration expiry date.

77. A method for combating spam according to any of claims 73 - 76 and wherein said classifying comprises inspecting whether registration of said registered address has expired.

30

78. A method for combating spam according to any of claims 73 - 76 and wherein said classifying comprises inspecting whether said registered address has not been registered.

5 79. A method for combating spam according to claim 75 and wherein said classifying comprises comparing said registration date to a predefined date.

80. A method for combating spam according claim 79 and wherein said predefined date is a current date.

10

81. A method for combating spam according to any of claims 73 - 80 and wherein said registered address comprises an internet domain name.

82. A method for combating spam according claim 81 and wherein said  
15 internet domain name is parked.

83. A method for combating spam according to any of claims 73 - 82 and wherein said handling comprises at least one of:

20 forwarding said message to an addressee of said message;  
storing said message in a predefined storage area;  
deleting said message;  
rejecting said message;  
sending said message to an originator of said message; and  
delaying said message for a period of time and thereafter re-classifying  
25 said message.

84. A method for combating spam according to any of claims 73 - 83 and wherein said message comprises at least one of:

30 an e-mail;  
a network packet;  
a digital telecom message; and  
an instant messaging message.

85. A method for combating spam according to any of claims 73 – 84 and wherein said classifying also comprises at least one of:
- requesting feedback from an addressee of said message;
  - 5 evaluating compliance of said message with a predefined policy;
  - evaluating registration status of at least one registered address in said message;
  - analyzing a match among network references in said message;
  - analyzing a match between at least one translatable address in said
  - 10 message and at least one other network reference in said message;
  - at least partially actuating an unsubscribe feature in said message;
  - analyzing an unsubscribe feature in said message;
  - employing a variable criteria;
  - sending information to a server and receiving classification data based
  - 15 thereon;
  - employing classification data received from a server; and
  - employing stored classification data.
86. A method for combating spam comprising:
- 20 classifying a message at least partially by relating to a match among network references in said message, thereby providing a spam classification for said message; and
  - handling said message based on said spam classification.
87. A method for combating spam according to claim 86 and wherein said network references include at least one translatable network address and wherein said match is between at least one translatable network address and another at least one of said network references.
88. A method for combating spam according to claim 87 and wherein said at least one translatable network address comprises a registered network address.
- 30

89. A method for combating spam according to claim 87 and wherein said at least one translatable network address comprises an internet domain name.

90. A method for combating spam according to any of claims 87 – 89 and wherein said classifying also comprises translating said translatable network address, thereby providing a translated network address.

91. A method for combating spam according to any of claims 86 – 90 and wherein said handling comprises at least one of:

10 forwarding said message to an addressee of said message;  
storing said message in a predefined storage area;  
deleting said message;  
rejecting said message;  
sending said message to an originator of said message; and  
15 delaying said message for a period of time and thereafter re-classifying said message.

92. A method for combating spam according to any of claims 86 – 91 and wherein said message comprises at least one of:

20 an e-mail;  
a network packet;  
a digital telecom message; and  
an instant messaging message.

25 93. A method for combating spam according to any of claims 86 – 92 and wherein said classifying also comprises at least one of:

requesting feedback from an addressee of said message;  
evaluating compliance of said message with a predefined policy;  
evaluating registration status of at least one registered address in said  
30 message;  
analyzing a match among network references in said message;

analyzing a match between at least one translatable address in said message and at least one other network reference in said message;  
at least partially actuating an unsubscribe feature in said message;  
analyzing an unsubscribe feature in said message;  
5 employing a variable criteria;  
sending information to a server and receiving classification data based thereon;  
employing classification data received from a server; and  
employing stored classification data.

10

94. A system for combating spam comprising:  
a message evaluator, operative to evaluate a message using at least one message parameter, said at least one message parameter comprising at least one variable criterion;

15

a message classifier, operative to provide a spam classification of said message at least partially based on an output of said message evaluator; and  
a message handler, operative to handle said message based on said spam classification.

20

95. A system for combating spam according to claim 94 and wherein said at least one variable criterion comprises a criterion which changes over time.

25

96. A system for combating spam according to claim 94 or claim 95 and wherein said at least one variable criterion comprises a parameter template-defined function.

30

97. A system for combating spam according to any of claims 94 - 96 and wherein:

said message evaluator includes at least one gateway; and  
said message classifier includes at least one server; and  
said at least one server is operative to receive said output from said at least one gateway and to provide said spam classification to said at least one gateway.

98. A system for combating spam according to claim 97 and wherein said at least one gateway also comprises:
- an encrypter, operative to encrypt at least part of said output by
  - 5 employing a non-reversible encryption so as to generate encrypted information; and
  - a transmitter, operative to transmit at least said encrypted information to said at least one server.
99. A system for combating spam according to claim 98 and wherein said
- 10 transmitter is operative to transmit information of a length limited to a predefined threshold.
100. A system for combating spam according to any of claims 94 - 99 and wherein said message handler is operative to perform at least one of the following:
- 15 forward said message to an addressee of said message;
  - store said message in a predefined storage area;
  - delete said message;
  - reject said message;
  - send said message to an originator of said message; and
  - 20 delay said message for a period of time and thereafter re-classify said message.
101. A system for combating spam according to any of claims 94 - 100 and wherein said message comprises at least one of:
- 25 an e-mail;
  - a network packet;
  - a digital telecom message; and
  - an instant messaging message.
- 30 102. A system for combating spam according to any of claims 94 - 101 and wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:



- feedback requested from an addressee of said message;  
compliance of said message with a predefined policy;  
a registration status of at least one registered address in said message;  
a match among network references in said message;  
5 a match between at least one translatable address in said message and at least one other network reference in said message;  
at least partial actuation of an unsubscribe feature in said message;  
an analysis of an unsubscribe feature in said message;  
a variable criteria;  
10 information sent to a server and classification data received based on said information;  
classification data received from a server; and  
stored classification data.
- 15 103. A system for combating spam comprising:  
a message evaluator, operative to evaluate multiple messages using at least one message parameter of said multiple messages, said at least one message parameter comprising at least one variable criterion which changes over time;  
a message classifier, operative to provide spam classifications of said  
20 messages at least partially based on outputs of said message evaluator; and  
a message handler, operative to handle said messages based on said spam classifications.
104. A system for combating spam according to claim 103 and wherein said  
25 spam classifications are at least partially based on similarities between plural messages among said multiple messages, which similarities are reflected in said at least one message parameter.
105. A system for combating spam according to claim 103 or claim 104 and  
30 wherein said spam classifications are at least partially based on similarities between plural messages among said multiple messages, which similarities are reflected in

outputs of applying said at least one evaluation criterion to said at least one message parameter.

106. A system for combating spam according to any of claims 103 - 105 and  
5 wherein said spam classifications are at least partially based on similarities in multiple outputs of applying a single evaluation criterion to said at least one message parameter in multiple messages.

107. A system for combating spam according to any of claims 103 - 106 and  
10 wherein said spam classifications are at least partially based on the extent of similarities between plural messages among said multiple messages which similarities are reflected in said at least one message parameter.

108. A system for combating spam according to any of claims 103 - 107 and  
15 wherein said spam classifications are at least partially based on the extent of similarities between plural messages among said multiple messages which similarities are reflected in outputs of applying said at least one evaluation criterion to said at least one message parameter.

20 109. A system for combating spam according to any of claims 103 - 108 and wherein said spam classifications are at least partially based on the extent of similarities in multiple outputs of applying a single evaluation criterion to said at least one message parameter in multiple messages.

25 110. A system for combating spam according to any of claims 107 - 109 and wherein said extent of similarities comprises a count of messages among said multiple messages which are similar.

111. A system for combating spam according to any of claims 103 - 110 and  
30 wherein said spam classifications are at least partially based on similarities in outputs of applying evaluation criteria to said at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to said at

least one message parameter in said multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of similarities among said multiple messages.

5 112. A system according to claim 111 and wherein said message classifier also comprises an aggregator, operative to aggregate individual similarities among said plurality of similarities.

113. A system according to claim 112 and wherein said aggregator is  
10 operative to apply a weighting to said individual similarities.

114. A system according to claim 112 and wherein said aggregator is operative to calculate a polynomial over said individual similarities.

15 115. A system for combating spam according to any of claims 103 - 114 and wherein said spam classifications are at least partially based on extents of similarities in outputs of applying evaluation criteria to said at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to said at least one message parameter in said multiple messages, yielding a corresponding  
20 plurality of outputs indicating a corresponding plurality of extents of similarities among said multiple messages.

116. A system according to claim 115 and wherein said message classifier also comprises an aggregator, operative to aggregate individual extents of similarities  
25 among said plurality of extents of similarities.

117. A system according to claim 116 and wherein said aggregator is operative to apply a weighting to said individual extents similarities.

30 118. A system according to claim 116 and wherein said aggregator is operative to calculate a polynomial over said individual extents of similarities.

119. A system for combating spam according to any of claims 115 - 118 and wherein said extents of similarities comprise a count of messages among said multiple messages which are similar.

5 120. A system for combating spam according to any of claims 103 - 119 and wherein said at least one variable criterion comprises a parameter template-defined function.

121. A system for combating spam according to any of claims 103 - 120 and  
10 wherein said message classifier is operative to employ a function of outputs of evaluating at least one message parameter of said multiple messages.

122. A system for combating spam according to claim 121 and wherein said spam classifications are at least partially based on similarities between outputs of said  
15 evaluating at least one message parameter of multiple messages.

123. A system for combating spam according to any of claims 103 - 122 and wherein:

said message evaluator includes at least one gateway;  
20 said message classifier includes at least one server; and  
said at least one server is operative to receive said outputs from said at least one gateway and to provide said spam classifications to said at least one gateway.

124. A system for combating spam according to claim 123 and wherein said at  
25 least one gateway also comprises:

an encrypter, operative to encrypt at least part of said outputs by employing a non-reversible encryption so as to generate encrypted information; and  
a transmitter, operative to transmit at least said encrypted information to  
said at least one server.

30

125. A system for combating spam according to claim 124 and wherein said transmitter is operative to transmit information of a length limited to a predefined threshold.

5 126. A system for combating spam according to any of claims 103 - 125 and wherein said message handler is operative to perform at least one of the following:

forward at least one of said messages to an addressee of said at least one of said messages;

store at least one of said messages in a predefined storage area;

10 delete at least one of said messages;

reject at least one of said messages;

send at least one of said messages to an originator of said at least one of said messages; and

15 delay at least one of said messages for a period of time and thereafter re-classify said at least one of said messages.

127. A system for combating spam according to any of claims 103 - 126 and wherein said messages comprise at least one of:

e-mail messages;

20 network packets;

digital telecom messages; and

instant messaging messages.

128. A system for combating spam according to any of claims 103 - 127 and  
25 wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:

feedback requested from addressees of said messages;

compliance of said messages with a predefined policy;

a registration status of at least one registered address in said messages;

30 a match among network references in said messages;

a match between at least one translatable address in said messages and at least one other network reference in said messages;

at least partial actuation of an unsubscribe feature in said messages;  
an analysis of an unsubscribe feature in said messages;  
a variable criteria;  
information sent to a server and classification data received based on said  
5 information;  
classification data received from a server; and  
stored classification data.

129. A system for combating spam comprising:  
10 a message categorizer, operative to categorize incoming messages  
received at at least one gateway into at least first, second and third categories; and  
a message classifier, operative to provide spam classifications for  
incoming messages in at least said first and second categories, said message classifier  
being operative to store incoming messages in said third category and at a time  
15 thereafter to provide spam classifications for said incoming messages in said third  
category.

130. A system for combating spam according to claim 129 and also  
comprising a message handler, operative to handle said incoming messages based on  
20 said spam classifications.

131. A system for combating spam according to claim 130 and wherein said  
message handler is operative to perform at least one of the following:  
forward at least one of said messages to an addressee of said at least one  
25 of said messages;  
store at least one of said messages in a predefined storage area;  
delete at least one of said messages;  
reject at least one of said messages;  
send at least one of said messages to an originator of said at least one of  
30 said messages; and  
delay at least one of said messages for a period of time and thereafter re-  
classify said at least one of said messages.

132. A system for combating spam according to any of claims 129 - 131 and wherein said message classifier is operative to provide a spam classification for a second message received at said at least one gateway at said time thereafter.

5

133. A system for combating spam according to any of claims 129 - 132 and wherein said time thereafter comprises a time not later than after a maximum predetermined waiting period.

10 134. A system for combating spam according to any of claims 129 - 133 and wherein said incoming messages comprise at least one of:

e-mail messages;  
network packets;  
digital telecom messages; and  
15 instant messaging messages.

135. A system for combating spam according to any of claims 129 - 135 and wherein said message categorizer is operative to categorize said messages at least partially based on at least one of the following:

20 feedback requested from addressees of said messages;  
compliance of said messages with a predefined policy;  
a registration status of at least one registered address in said messages;  
a match among network references in said messages;  
a match between at least one translatable address in said messages and at  
25 least one other network reference in said messages;  
at least partial actuation of an unsubscribe feature in said messages;  
an analysis of an unsubscribe feature in said messages;  
a variable criteria;  
information sent to a server and classification data received based on said  
30 information;  
categorization data received from a server; and  
stored categorization data.

136. A system for combating spam according to any of claims 129 – 135 and wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:

- 5 feedback requested from addressees of said messages;
- compliance of said messages with a predefined policy;
- a registration status of at least one registered address in said messages;
- a match among network references in said messages;
- a match between at least one translatable address in said messages and at
- 10 least one other network reference in said messages;
- at least partial actuation of an unsubscribe feature in said messages;
- an analysis of an unsubscribe feature in said messages;
- a variable criteria;
- information sent to a server and classification data received based on said
- 15 information;
- classification data received from a server; and
- stored classification data.

137. A system for combating spam comprising:

- 20 a message classifier, operative to provide a spam classification for a message at least partially by relating to an unsubscribe feature in said message; and
- a message handler, operative to handle said message based on said spam classification.

25 138. A system for combating spam according to claim 137 and also comprising an unsubscribe identifier, operative to identify whether said message includes an unsubscribe feature.

139. A system for combating spam according to claim 137 or claim 138 and  
30 also comprising an addressee identifier, operative to identify whether said unsubscribe feature includes a reference to an addressee of said message.



140. A system for combating spam according to claim 139 and wherein said reference to an addressee of said message comprises an e-mail address.

141. A system for combating spam according to claim 139 and wherein said  
5 reference to an addressee of said message comprises a per-addressee generated ID.

142. A system for combating spam according to claim 141 and wherein said per-addressee generated ID comprises a user identification number.

10 143. A system for combating spam comprising:  
a message classifier, operative to provide a spam classification for a message at least partially by at least partial actuation of an unsubscribe feature in the message; and  
a message handler, operative to handle said message based on said spam  
15 classification.

144. A system for combating spam according to claim 143 and also comprising an actuation analyzer operative to analyze an output of said at least partial actuation.

20 145. A system for combating spam according to claim 144 and wherein said analyzer is operative to sense whether part of said output indicates the occurrence of an error.

25 146. A system for combating spam according to claim 145 and wherein said at least partial actuation also comprises at least attempting communication with a network server.

147. A system for combating spam according to claim 146 and wherein said  
30 error indicates that said network server does not exist.

148. A system for combating spam according to claim 146 and wherein said error indicates that said network server does not provide an unsubscribe functionality.

149. A system for combating spam according to claim 146 and wherein said  
5 error indicates that said network server cannot unsubscribe a message addressee.

150. A system for combating spam according to claim 144 and wherein said analyzer is operative to sense whether part of said output comprises an addressee reference.

10

151. A system for combating spam according to claim 150 and wherein said addressee reference comprises an e-mail address.

152. A system for combating spam according to claim 150 and wherein said  
15 addressee reference comprises a per-addressee generated ID.

153. A system for combating spam according to claim 152 and wherein said per-addressee generated ID comprises a user identification number.

20 154. A system for combating spam according to any of claims 150 - 153 and wherein said analyzer is operative to relate said addressee reference to at least one addressee reference characteristic of said message.

155. A system for combating spam according to claim 154 and wherein said at  
25 least one addressee reference characteristic of said message comprises an e-mail address.

156. A system for combating spam according to claim 154 and wherein said at  
30 least one addressee reference characteristic of said message comprises a per-addressee generated ID.

157. A system for combating spam according to claim 156 and wherein said per- at least one addressee reference characteristic of said per-addressee generated ID comprises a user identification number.

5 158. A system for combating spam according to any of claims 137 – 157 and also comprising an unsubscribe recognizer, operative to recognize said unsubscribe feature.

159. A system for combating spam according to claim 158 and wherein said  
10 unsubscribe recognizer is operative to sense a part of said message comprising predefined keywords.

160. A system for combating spam according to claim 159 and wherein said  
15 unsubscribe recognizer is operative to sense a part of said message comprising a network reference and a reference to an addressee of said messages.

161. A system for combating spam according to claim 160 and wherein said network reference comprises a reference to a network server.

20 162. A system for combating spam according to claim 160 or claim 161 and wherein said reference to an addressee of said message comprises an addressee e-mail address.

163. A system for combating spam according to any of claims 137 – 162 and  
25 wherein said message handler is operative to perform at least one of the following:  
forward said message to an addressee of said message;  
store said message in a predefined storage area;  
delete said message;  
reject said message;  
30 send said message to an originator of said message; and  
delay said message for a period of time and thereafter re-classify said message.

164. A system for combating spam according to any of claims 137 – 163 and wherein said message comprises at least one of:

- an e-mail;
- 5 a network packet;
- a digital telecom message; and
- an instant messaging message.

165. A system for combating spam according to any of claims 137 – 164 and wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:

- feedback requested from an addressee of said message;
- compliance of said message with a predefined policy;
- a registration status of at least one registered address in said message;
- 15 a match among network references in said message;
- a match between at least one translatable address in said message and at least one other network reference in said message;
- at least partial actuation an unsubscribe feature in said message;
- an analysis of an unsubscribe feature in said message;
- 20 a variable criteria;
- information sent to a server and classification data received based on said information;
- classification data received from a server; and
- stored classification data.

25 166. A system for combating spam comprising:  
a message classifier, operative to provide a spam classification for a message at least partially by relating to registration status of at least one registered address in said message; and  
30 a message handler, operative to handle said message based on said spam classifications.

167. A system for combating spam according to claim 166 and wherein said message classifier is operative to employ a network service for determining said registration status.

5 168. A system for combating spam according to claim 166 or claim 167 and wherein said registration status comprises a registration date.

169. A system for combating spam according to claim 166 or claim 167 and wherein said registration status comprises a registration expiry date.

10 170. A system for combating spam according to any of claims 166 - 169 and wherein said message classifier is operative to inspect whether registration of said registered address has expired.

15 171. A system for combating spam according to any of claims 166 - 169 and wherein said message classifier is operative to inspect whether said registered address has not been registered.

20 172. A system for combating spam according to claim 168 and wherein said message classifier is operative to compare said registration date to a predefined date.

173. A system for combating spam according claim 172 and wherein said predefined date is a current date.

25 174. A system for combating spam according to any of claims 166 – 173 and wherein said registered address comprises an Internet domain name.

175. A system for combating spam according claim 174 and wherein said Internet domain name is parked.

30 176. A system for combating spam according to any of claims 166 – 175 and wherein said message handler is operative to perform at least one of the following:

forward said message to an addressee of said message;  
store said message in a predefined storage area;  
delete said message;  
reject said message;  
5 send said message to an originator of said message; and  
delay said message for a period of time and thereafter re-classify said  
message.

177. A system for combating spam according to any of claims 166 – 176 and  
10 wherein said message comprises at least one of:  
an e-mail;  
a network packet;  
a digital telecom message; and  
an instant messaging message.

15  
178. A system for combating spam according to any of claims 166 – 177 and  
wherein said message classifier is operative to provide said spam classification at least  
partially based on at least one of the following:  
feedback requested from an addressee of said message;  
20 compliance of said message with a predefined policy;  
a registration status of at least one registered address in said message;  
a match among network references in said message;  
a match between at least one translatable address in said message and at  
least one other network reference in said message;  
25 at least partial actuation an unsubscribe feature in said message;  
an analysis of an unsubscribe feature in said message;  
a variable criteria;  
information sent to a server and classification data received based on said  
information;  
30 classification data received from a server; and  
stored classification data.

179. A system for combating spam comprising:

a message classifier, operative to provide a spam classification for a message at least partially by relating to a match among network references in said message; and

5 a message handler, operative to handle said message based on said spam classification.

180. A system for combating spam according to claim 179 and wherein said network references include at least one translatable network address and wherein said  
10 match is between at least one translatable network address and another at least one of said network references.

181. A system for combating spam according to claim 180 and wherein said at least one translatable network address comprises a registered network address.

15

182. A system for combating spam according to claim 180 and wherein said at least one translatable network address comprises an Internet domain name.

183. A system for combating spam according to any of claims 180 – 182 and  
20 also comprising an address translator, operative to translate said translatable network address, thereby providing a translated network address.

184. A system for combating spam according to any of claims 179 – 183 and wherein said message handler is operative to perform at least one of the following:

25

forward said message to an addressee of said message;

store said message in a predefined storage area;

delete said message;

reject said message;

send said message to an originator of said message; and

30

delay said message for a period of time and thereafter re-classify said message.

185. A system for combating spam according to any of claims 179 – 184 and wherein said message comprises at least one of:

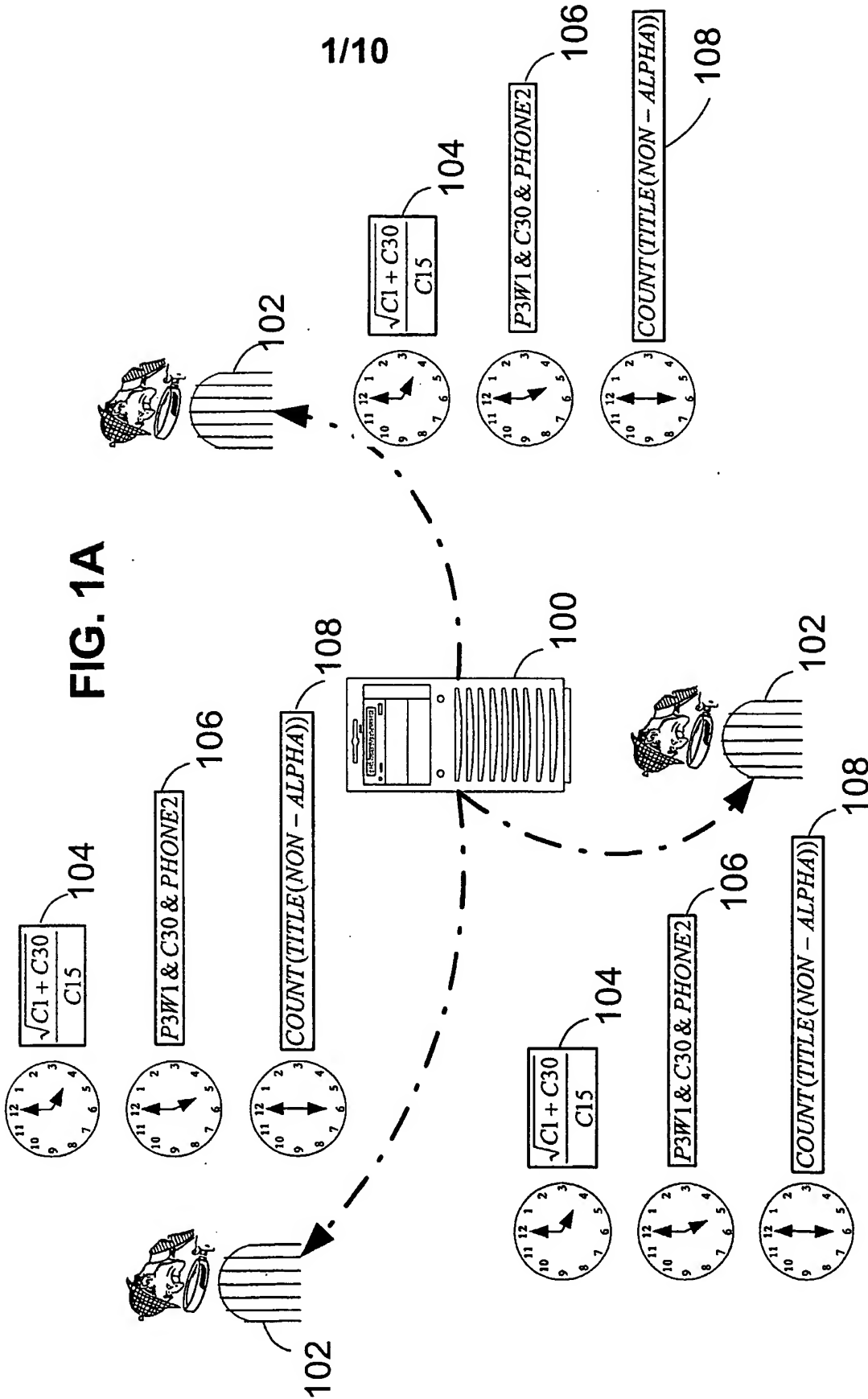
- an e-mail;
- a network packet;
- 5 a digital telecom message; and
- an instant messaging message.

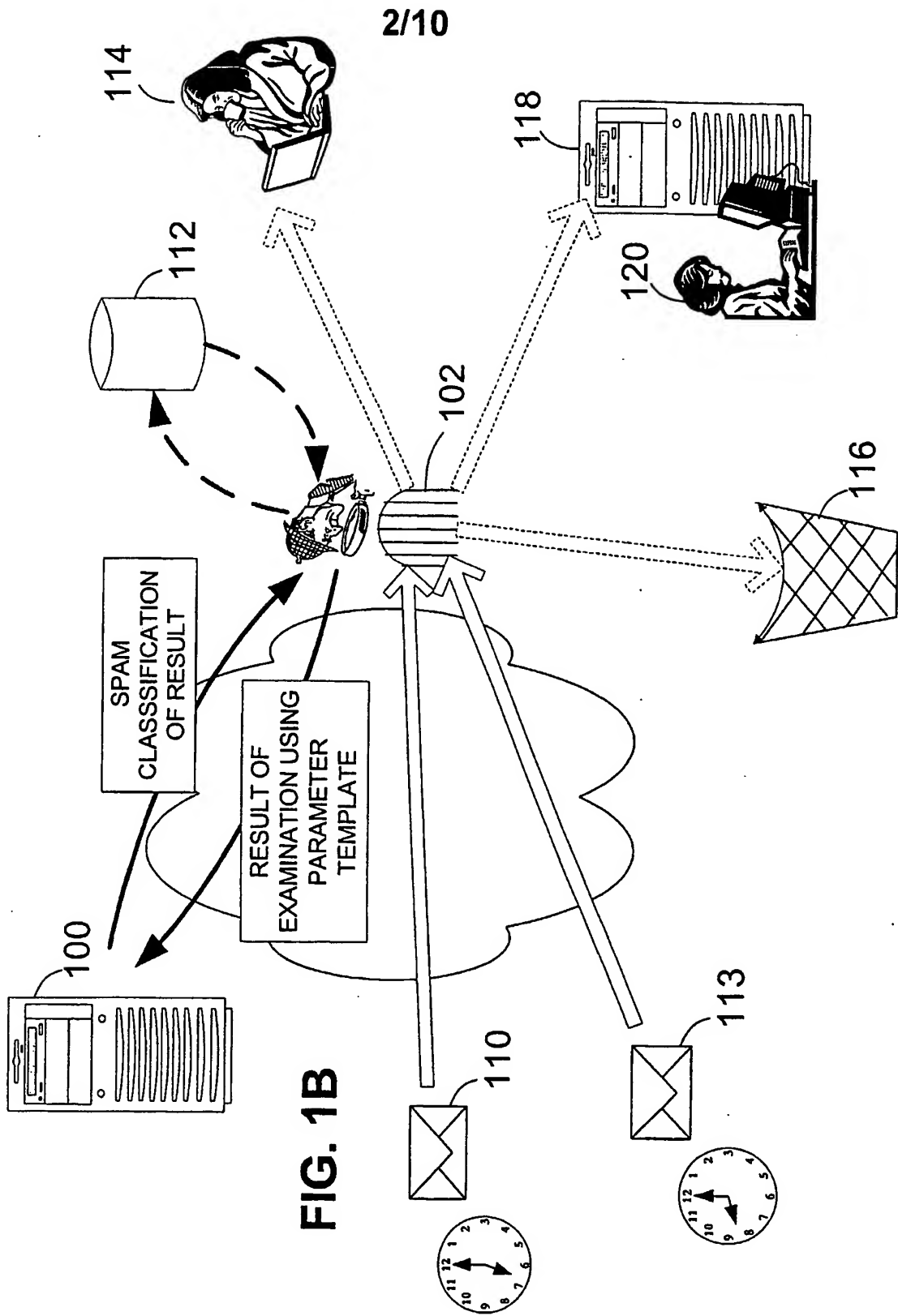
186. A system for combating spam according to any of claims 179 – 185 and wherein said message classifier is operative to provide said spam classification at least  
10 partially based on at least one of the following:

- feedback requested from an addressee of said message;
- compliance of said message with a predefined policy;
- a registration status of at least one registered address in said message;
- a match among network references in said message;
- 15 a match between at least one translatable address in said message and at least one other network reference in said message;
- at least partial actuation an unsubscribe feature in said message;
- an analysis of an unsubscribe feature in said message;
- a variable criteria;
- 20 information sent to a server and classification data received based on said information;
- classification data received from a server; and
- stored classification data.

25







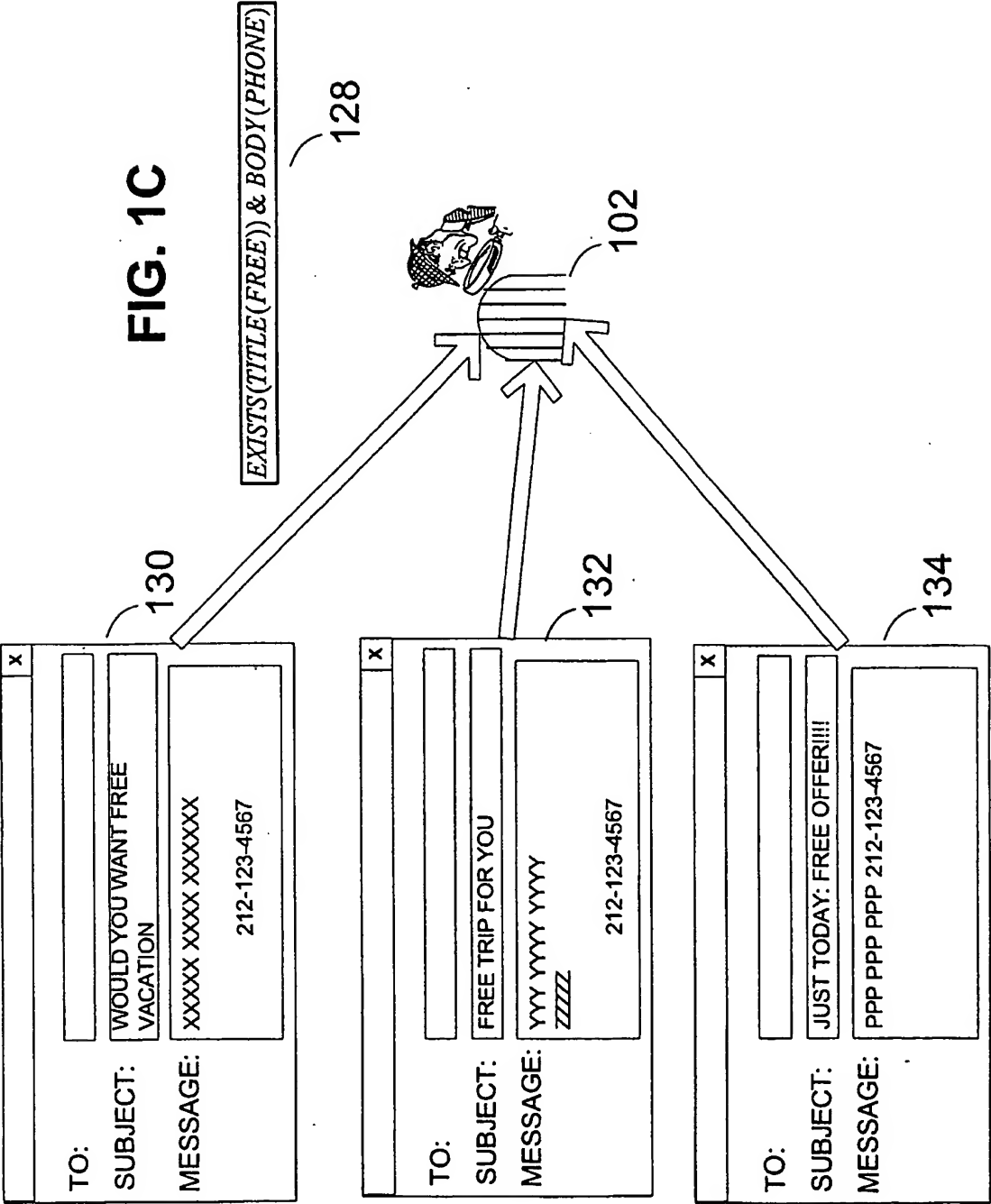
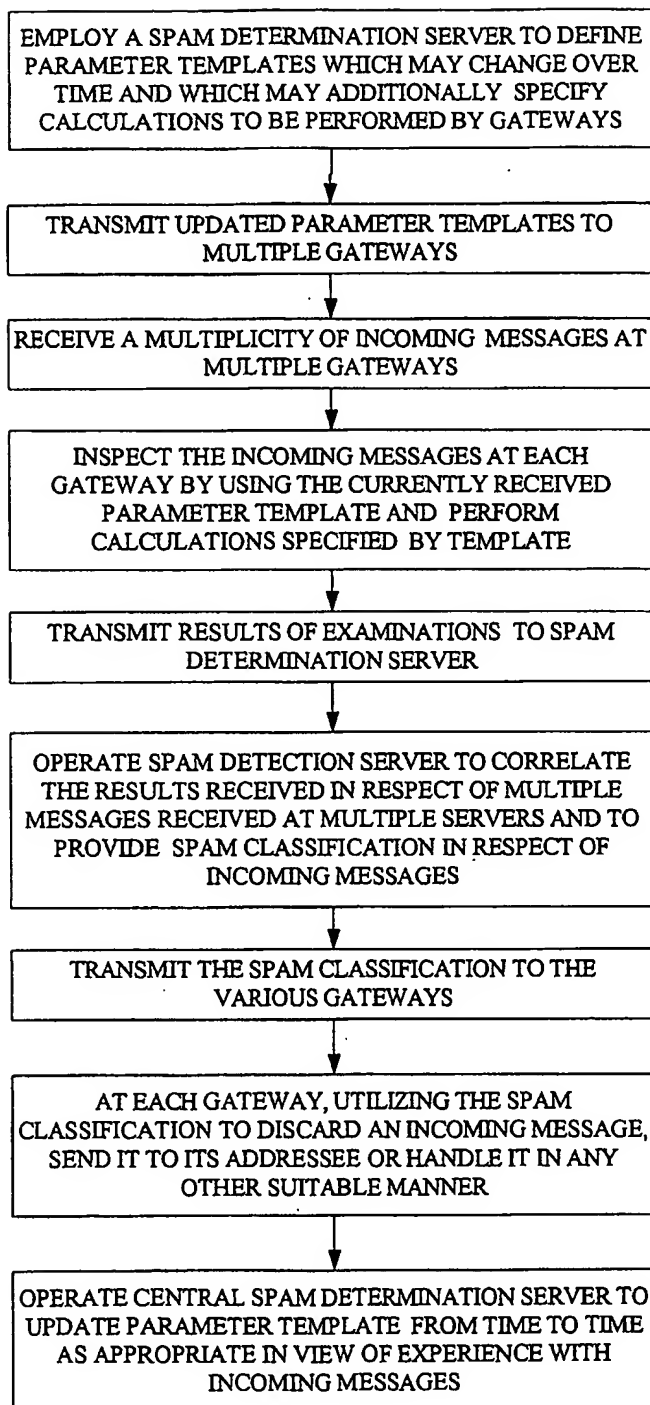


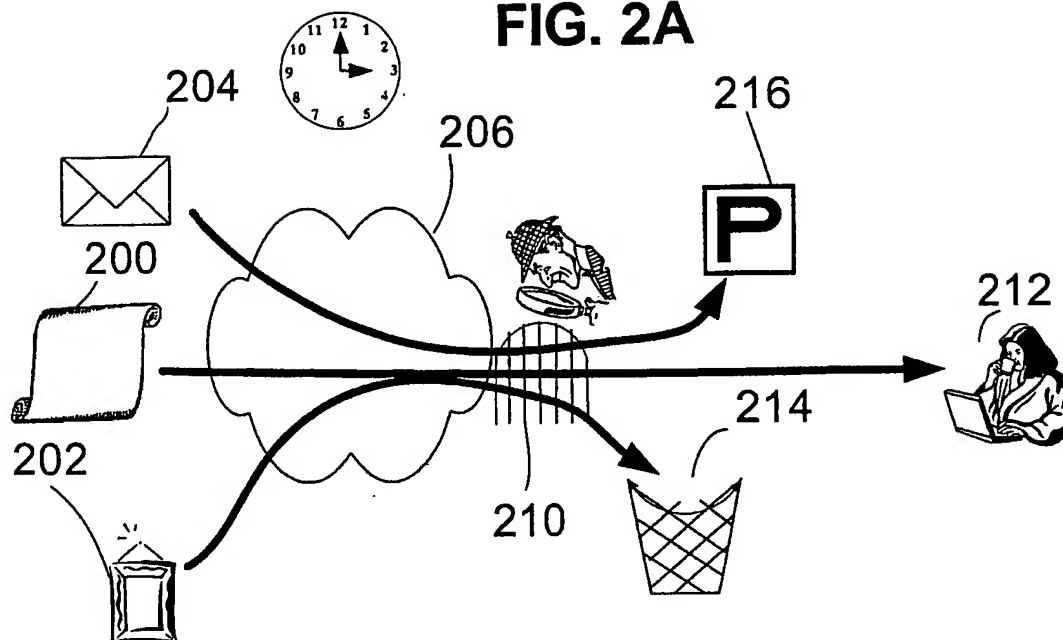
FIG. 1D

4/10

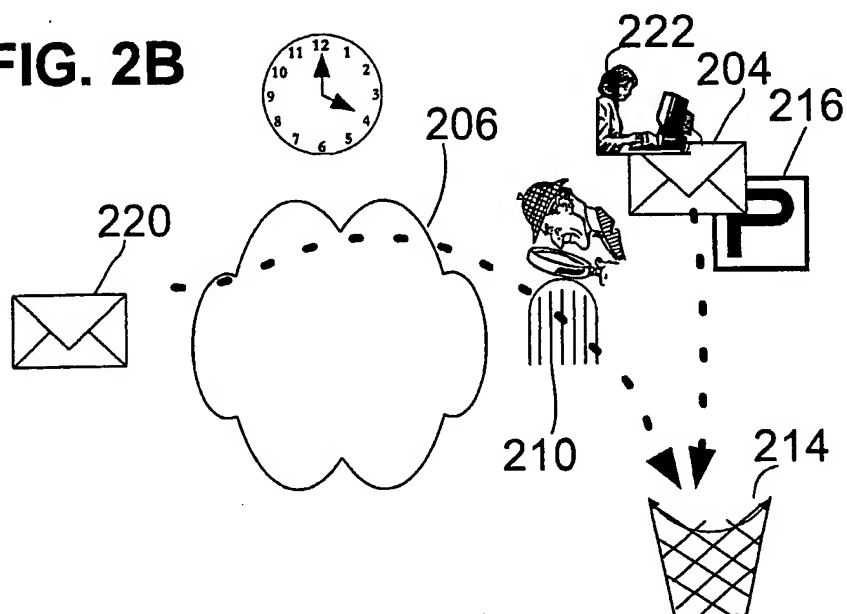


**5/10**

**FIG. 2A**

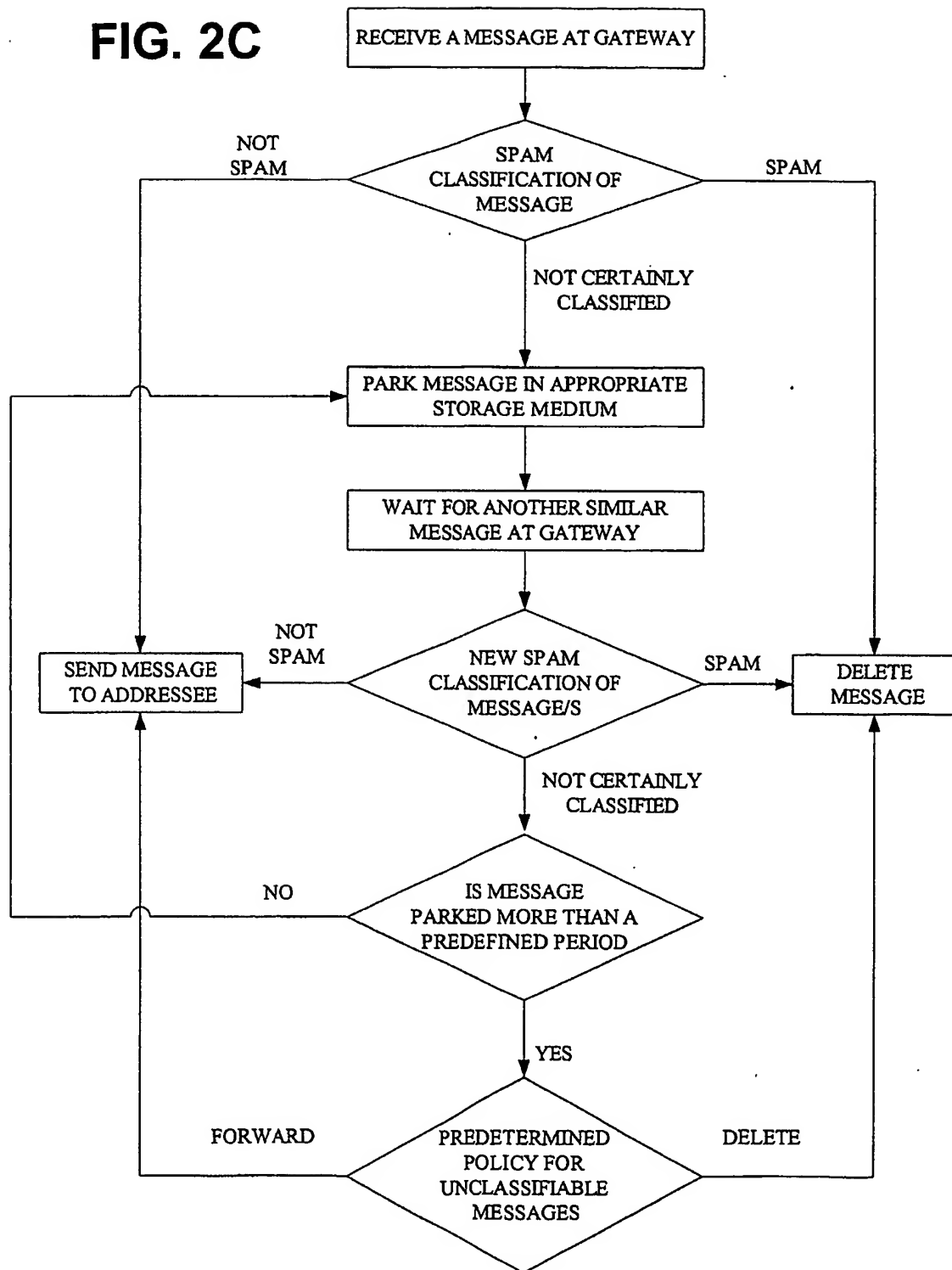


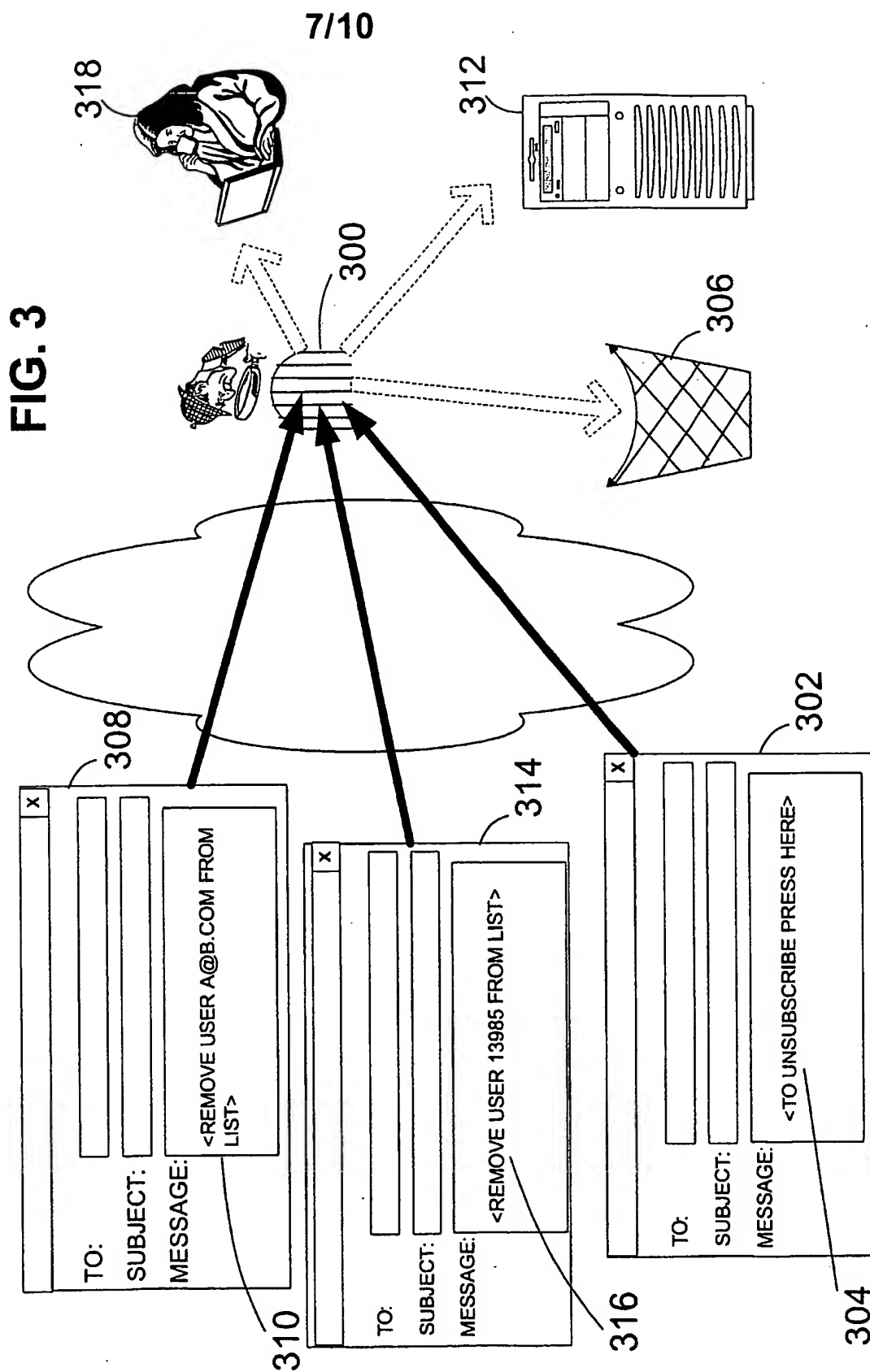
**FIG. 2B**



6/10

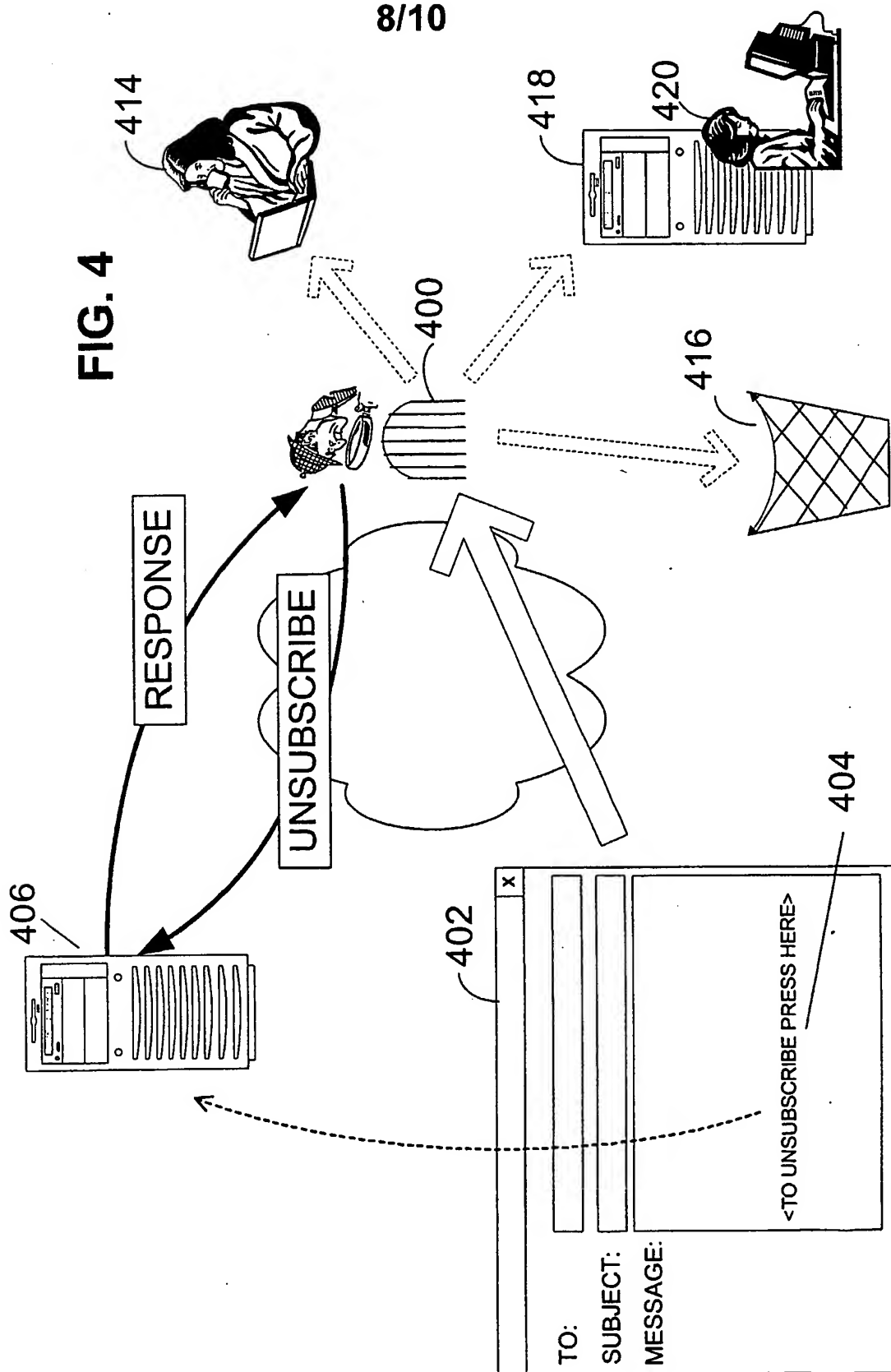
FIG. 2C



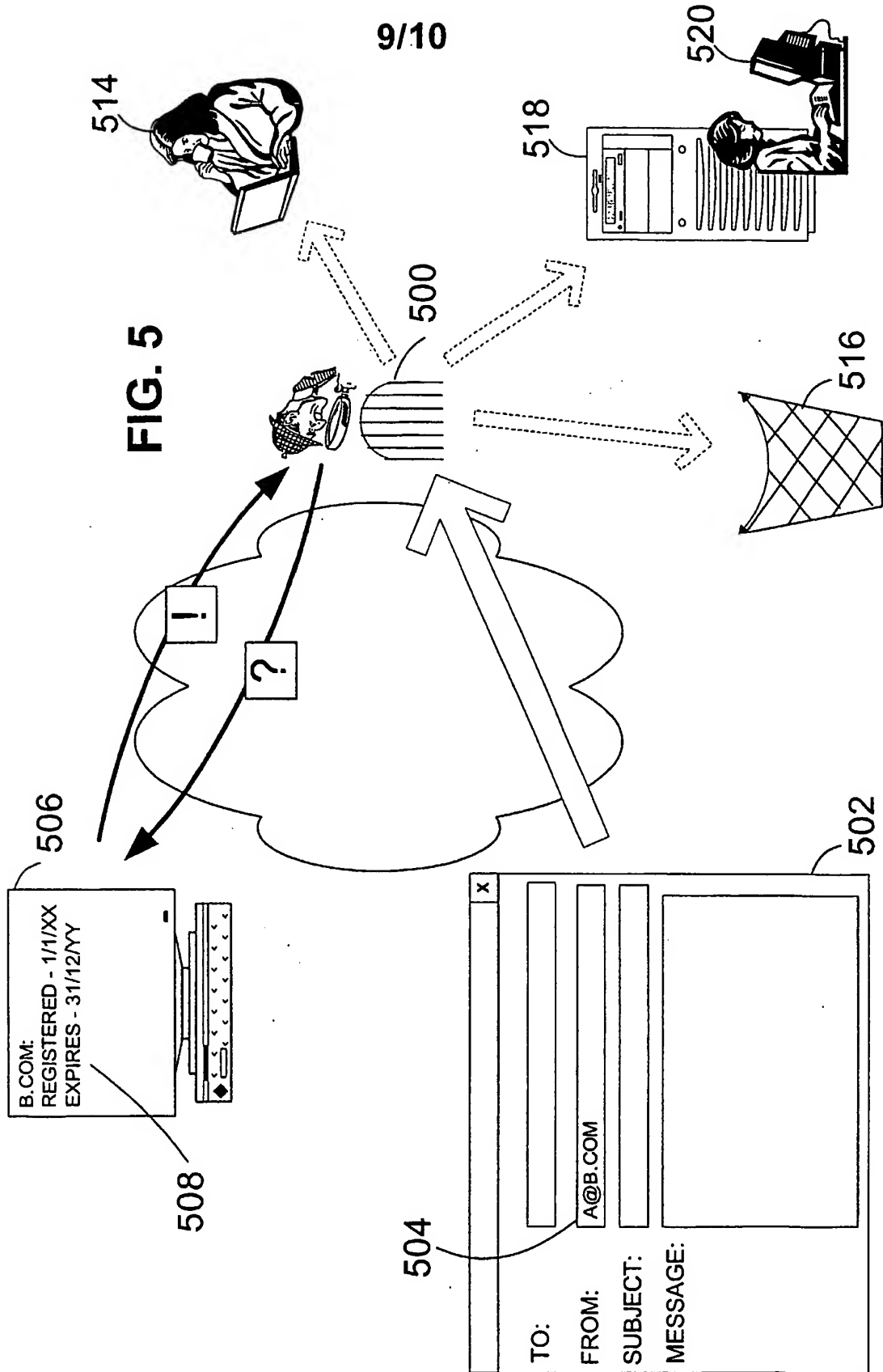


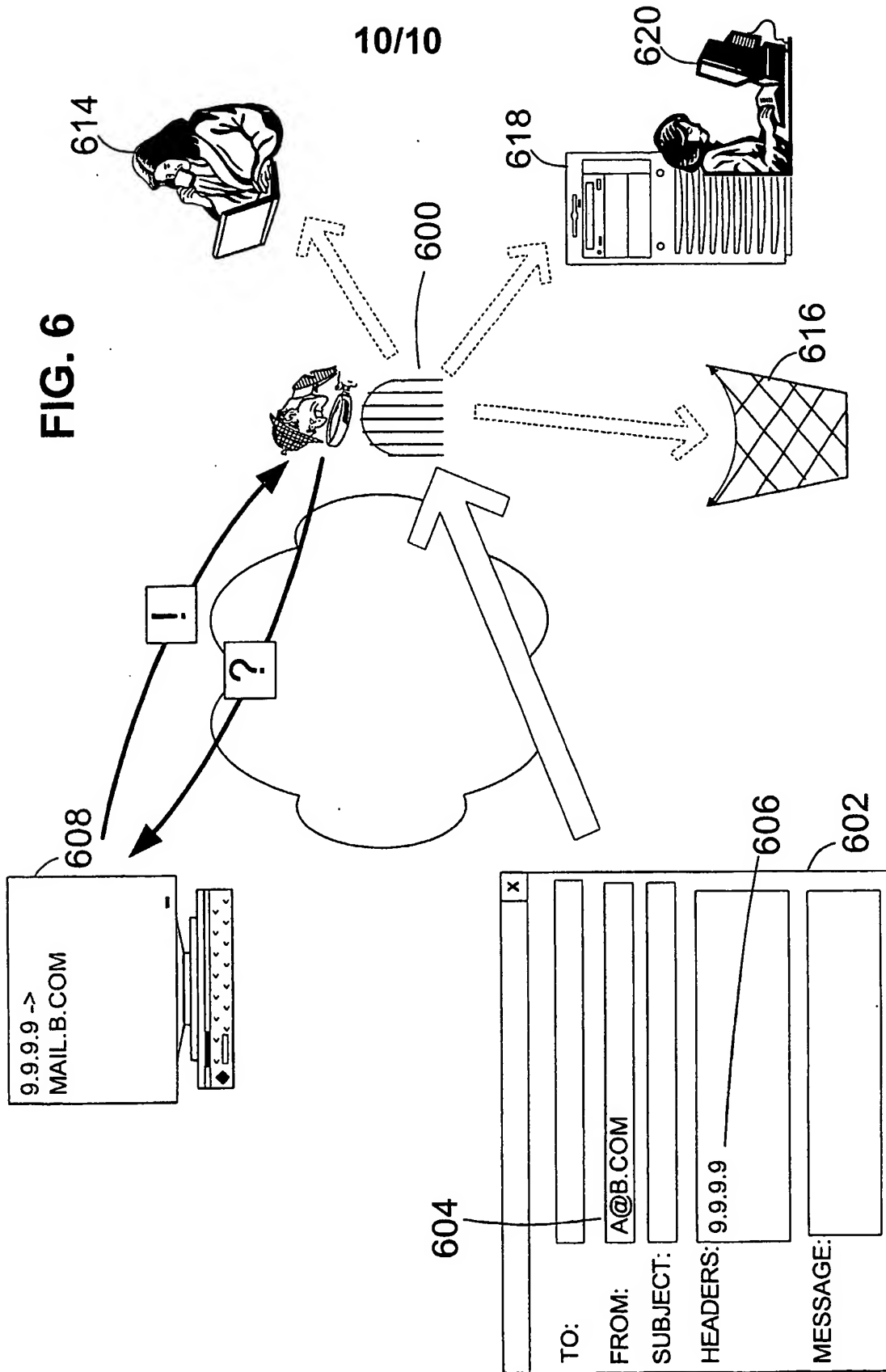
8/10

FIG. 4









# INTERNATIONAL SEARCH REPORT

International application No.

PCT/IL03/01103

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 15/173, 11/30, 12/14; H04L 09/00, 09/32

US CL : 709/206; 713/200, 201

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/206; 713/200, 201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
Please See Continuation Sheet

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	JP 2003348162 A (NEC CORP.) 05 December 2003 (05.12.2003), see Abstract.	1-186
A,P	JP 2003099372 A (EIJITSU LTD.) 04 April 2003 (04.04.2003), see Abstract.	1-186
A,P	JP 2003099371 A (TOSHIBA CORP.) 04 April 2003 (04.04.2003), see Abstract.	1-186
A,P	JP 2003087327 A (SHARP CORP.) 20 March 2003 (20.03.2003), see Abstract.	1-186
A,P	WO 03/054,764 A1(LEE et al.) 03 July 2003 (03.07.2003), see Abstract.	1-186
A,T	US 6,687,740 B1 (GOUGH et al.) 03 February 2004 (03.02.2004), column 2, line 14-52.	1-186
A,T	US 6,691,156 B1 (DRUMMOND et al.) 10 February 2004 (10.02.2004), column 2, line 23 to column 3, line 37.	1-186
A,P	US 6,615,241 B1 (MILLER et al.) 02 September 2003 (02.09.2003), column 5, lines 14-38; column 6, lines 26-38.	1-186
A	US 6,330,590 B1 (COTTEN) 11 December 2001 (11.12.2001), column 3, line 6 to column 5, line 23.	1-186



Further documents are listed in the continuation of Box C.



See patent family annex.

Special categories of cited documents:		"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"B"	earlier application or patent published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search

24 May 2004 (24.05.2004)

Date of mailing of the international search report

03 JUN 2004

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US  
Commissioner for Patents

P.O. Box 1450  
Alexandria, Virginia 22313-1450

Facsimile No. (703)305-3230

Authorized officer

Ayaz Sheikh

Telephone No. (703)305-3900

# INTERNATIONAL SEARCH REPORT

PCT/IL03/01103

## C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,161,130 A (HORVITZ et al.) 12 December 2000 (12.12.2000), column 4, line 40 to column 6, line 4; column 8, line 40 to column 9, line 51; column 10, lines 38-49; column 11, line 55 to column 12, line 52; column 13, line 29-57; column 14, line 1-58; column 15, line 30 to column 16, line 67.	1-186

**INTERNATIONAL SEARCH REPORT**

PCT/IL03/01103

**Continuation of B. FIELDS SEARCHED Item 3:**

IEEE, EAST, ACM

search terms: spam, junk, e-mail, unwanted, unsolicited, messages